Euroopa Liidu
Nõukogu

Brüssel, 3. märts 2021
(OR. en)

14308/20

Institutsioonidevaheline
dokument:
2018/0331 (COD)

CT 122
ENFOPOL 355
COTER 121
JAI 1135
CYBER 285
TELECOM 281
FREMP 149
AUDIO 70
DROIPEN 127
CODEC 1412

SEADUSANDLIKUD AKTID JA MUUD DOKUMENDID

Teema:	Nõukogu esimese lugemise seisukoht eesmärgiga võtta vastu EUROOPA PARLAMENDI JA NÕUKOGU MÄÄRUS, mis käsitleb võitlemist terroristliku veebisisu levitamise vastu

EUROOPA PARLAMENDI JA NÕUKOGU

MÄÄRUS (EL) 2021/…,

…,

mis käsitleb võitlemist terroristliku veebisisu levitamise vastu

EUROOPA PARLAMENT JA EUROOPA LIIDU NÕUKOGU,

võttes arvesse Euroopa Liidu toimimise lepingut, eriti selle artiklit 114,

võttes arvesse Euroopa Komisjoni ettepanekut,

olles edastanud seadusandliku akti eelnõu liikmesriikide parlamentidele,

võttes arvesse Euroopa Majandus- ja Sotsiaalkomitee arvamust,[1]

toimides seadusandliku tavamenetluse kohaselt[2]

[1] ELT C 110, 22.3.2019, lk 67.

[2] Euroopa Parlamendi 17. aprilli 2019. aasta seisukoht (*Euroopa Liidu Teatajas* seni avaldamata) ja nõukogu … esimese lugemise seisukoht (*Euroopa Liidu Teatajas* seni avaldamata). Euroopa Parlamendi … seisukoht (*Euroopa Liidu Teatajas* seni avaldamata).

ning arvestades järgmist:

(1) Käesoleva määruse eesmärk on tagada veebimajutusteenuste terrorismi eesmärgil kuritarvitamise vastu võitlemisega ja liidu avalikule julgeolekule kaasaaitamisega digitaalse ühtse turu sujuv toimimine avatud ja demokraatlikus ühiskonnas. Digitaalse ühtse turu toimimist tuleks parandada järgmiste meetmetega: suurema õiguskindluse tagamine veebimajutusteenuse pakkujatele, kasutajate usalduse suurendamine veebikeskkonna vastu ning väljendusvabaduse, sealhulgas avatud ja demokraatlikus ühiskonnas teabe ja ideede saamise ja edastamise vabaduse ning meediavabaduse ja meedia mitmekesisuse tagatiste tugevdamine.

(2) Terroristliku veebisisu levitamise vastu võitlemist reguleerivaid meetmeid peaksid täiendama liikmesriikide terrorismivastase võitluse strateegiad, mis hõlmavad meediapädevuse ja kriitilise mõtlemise tugevdamist, alternatiivsete narratiivide ja vastupropaganda arendamist ning muid algatusi terroristliku veebisisu mõju ja sellega seotud kaitsetuse vähendamiseks, samuti investeerimist sotsiaaltöösse, deradikaliseerimisalgatusi ja koostööd mõjutatud kogukondadega, et ühiskonnas radikaliseerumist jätkusuutlikult ennetada.

(3) Terroristliku veebisisu, mis on osa laiemast ebaseadusliku veebisisu probleemist, levitamise vastu võitlemiseks on vaja kombineerida seadusandlikud, muud kui seadusandlikud ja vabatahtlikud meetmed ametiasutuste ja veebimajutusteenuse pakkujate koostöös viisil, millega austatakse täiel määral põhiõigusi.

(4) Veebis aktiivselt tegutsevad veebimajutusteenuse pakkujad mängivad digimajanduses olulist rolli: nad viivad kokku ettevõtted ja kodanikud, lihtsustavad avalikke arutelusid ning teabe, arvamuste ja ideede levitamist ja vastuvõttu, andes seega olulise panuse innovatsiooni, majanduskasvu ja töökohtade loomisse liidus. Paraku kuritarvitavad kolmandad isikud mõningatel juhtudel veebimajutusteenuse pakkujate teenuseid, et panna veebis toime ebaseaduslikke tegusid. Eriti murelikuks teeb see, kui neid teenuseid kuritarvitavad terroristlikud rühmitused ja nende toetajad, kes levitavad terroristlikku veebisisu oma sõnumi tutvustamiseks, inimeste radikaliseerimiseks ja uute liikmete värbamiseks ning terroristliku tegevuse juhtimiseks ja hõlbustamiseks.

(5) Kuigi see ei ole ainus tegur, on ilmnenud, et terroristlik veebisisu mõjub isikute radikaliseerumisel katalüsaatorina ning võib kaasa tuua terroriakte, ning seega on sellel tõsised negatiivsed tagajärjed nii kasutajate, kodanike ja laiema ühiskonna kui ka nimetatud sisu majutavate veebiteenuste osutajate jaoks, sest see õõnestab nende kasutajate usaldust ja kahjustab nende ärimudeleid. Arvestades veebimajutusteenuse pakkujate keskset rolli ja nende osutatavate teenustega seotud tehnoloogilisi vahendeid ja võimalusi, on veebimajutusteenuse pakkujatel eriline ühiskondlik kohustus kaitsta oma teenuseid terroristidepoolse kuritarvitamise eest ning aidata võidelda terroristlikku sisu vastu, mida levitatakse nende teenuseid kasutades veebis, võttes samas arvesse väljendusvabaduse, sealhulgas avatud ja demokraatlikus ühiskonnas teabe ja ideede saamise ja edastamise vabaduse määravat tähtsust.

(6) Liidu tasandil alustati võitlust terroristliku veebisisu vastu 2015. aastal liikmesriikide ja veebimajutusteenuse pakkujate vabatahtliku koostööraamistiku alusel. Neid meetmeid tuleks täiendada selge õigusraamistikuga, et veelgi vähendada juurdepääsu terroristlikule veebisisule ja leida sellele kiirelt arenevale probleemile sobiv lahendus. Õigusraamistik tugineb vabatahtlikule tööle, mida komisjon on toetanud oma soovituses (EL) 2018/334,[1] ning see on vastus Euroopa Parlamendi üleskutsetele kasutada võitluses ebaseadusliku ja kahjuliku veebisisu vastu jõulisemaid meetmeid kooskõlas Euroopa Parlamendi ja nõukogu direktiivis 2000/31/EÜ[2] kehtestatud horisontaalse raamistikuga ja Euroopa Ülemkogu üleskutsetele parandada terroriaktidele õhutava veebisisu avastamist ja eemaldamist.

(7) Käesolev määrus ei tohiks mõjutada direktiivi 2000/31/EÜ kohaldamist. Ennekõike ei tohiks ükski meede, sealhulgas erimeede, mille veebimajutusteenuse pakkuja võtab kooskõlas käesoleva määrusega, takistada kõnealusel veebimajutusteenuse pakkujal kasutada nimetatud direktiivi kohast vastutusest vabastamise erandit. Veelgi enam, käesolev määrus ei mõjuta liikmesriikide ametiasutuste ja kohtute õigust teha kindlaks veebimajutusteenuse pakkuja vastutus, kui kõnealuses direktiivis sätestatud vastutusest vabastamise erandi tingimused ei ole täidetud.

---

1 Komisjoni 1. märtsi 2018. aasta soovitus (EL) 2018/334 meetmete kohta, millega tulemuslikult võidelda ebaseadusliku veebisisu vastu (ELT L 63, 6.3.2018, lk 50).

2 Euroopa Parlamendi ja nõukogu 8. juuni 2000. aasta direktiiv 2000/31/EÜ infoühiskonna teenuste teatavate õiguslike aspektide, eriti elektroonilise kaubanduse kohta siseturul (direktiiv elektroonilise kaubanduse kohta) (EÜT L 178, 17.7.2000, lk 1).

(8) Kui käesolev määrus on vastuolus direktiivi 2010/13/EL artikli 1 lõike 1 punktis a määratletud audiovisuaalmeedia teenuseid reguleerivate sätetega, peaks direktiiv 2010/13/EL olema ülimuslik. See ei tohiks mõjutada käesolevast määrusest tulenevaid kohustusi, eelkõige neid, mis on seotud videojagamisplatvormi teenuste osutajatega.

(9) Käesolevas määruses tuleks sätestada õigusnormid, mille abil võidelda veebimajutusteenuste kuritarvitamise vastu terroristliku veebisisu levitamisel, et tagada siseturu tõrgeteta toimimine. Nimetatud normid peaksid täiel määral austama liidus kaitstud põhiõigusi, eelkõige Euroopa Liidu põhiõiguste hartaga (edaspidi „harta“) tagatud õigusi.

(10) Käesoleva määruse eesmärk on aidata kaasa avaliku julgeoleku kaitsmisele kehtestades samas asjakohased ja kindlad meetmed, et kaitsta asjaomaseid põhiõigusi, muu hulgas õigust eraelu puutumatusele ja isikuandmete kaitsele, õigust väljendusvabadusele, sealhulgas vabadust saada ja edastada teavet, ettevõtlusvabadust ning õigust tõhusale õiguskaitsevahendile. Lisaks on keelatud igasugune diskrimineerimine. Pädevad asutused ja veebimajutusteenuse pakkujad peaksid võtma üksnes selliseid meetmeid, mis on demokraatlikus ühiskonnas vajalikud, asjakohased ja proportsionaalsed, võttes arvesse seda, kui oluliseks peetakse väljendus- ja teabevabadust, samuti meediavabadust ning meedia mitmekesisust, mis on pluralistliku ja demokraatliku ühiskonna põhialused ning liidu alusväärtused. Meetmed, mis mõjutavad väljendus- ja teabevabadust, peaksid terroristliku veebisisu levitamise vastu võitlemiseks olema rangelt sihipärased, samal ajal austades õigust seaduslikult teavet saada ja edastada, võttes arvesse veebimajutusteenuse pakkujate keskset rolli avalikule arutelule ning faktide, arvamuste ja ideede õiguspärasele levitamisele kaasaaitamisel. Tõhusad veebipõhised meetmed terroristliku veebisisu levitamise vastu võitlemiseks ning väljendus- ja teabevabaduse kaitse ei vastandu teineteisele, vaid täiendavad ja tugevdavad teineteist.

(11) Et oleks selge, milliseid meetmeid peaksid nii veebimajutusteenuse pakkujad kui ka pädevad asutused terroristliku veebisisu levitamise vastu võitlemiseks võtma, tuleks käesolevas määruses ennetavalt määratleda terroristlik sisu, kooskõlas Euroopa Parlamendi ja nõukogu direktiivis (EL) 2017/541[1] kasutatud asjaomaste kuritegude määratlusega. Arvestades, et tegeleda tuleb kõige kahjulikuma veebis leviva propaganda, nimelt terroristliku propagandaga, peaks see määratlus hõlmama materjali, mis õhutab või ärgitab kedagi terroriakte toime panema või nende toimepanemisele kaasa aitama või ärgitab kedagi osalema terrorirühmituse tegevuses või ülistab terroristlikku tegevust, sealhulgas terrorirünnakut kujutavat materjali. Määratlus peaks hõlmama ka materjali, mis annab suuniseid lõhkeainete, tulirelvade või muude relvade või kahjulike või ohtlike ainete, samuti keemiliste, bioloogiliste, radioloogiliste ja tuumaainete (KBRT-ained) valmistamiseks või kasutamiseks, või muude erimeetodite või tehnikate kohta, sealhulgas sihtmärkide valimiseks terroriaktide toimepanemise või nende toimepanemisele kaasaaitamise eesmärgil. Selline materjal on eelkõige tekst, kujutis, helisalvestis ja video, samuti terroriaktide otseülekanne, mis tekitab ohu, et selliseid kuritegusid võidakse korda saata ka edaspidi. Kui pädevad asutused või veebimajutusteenuse pakkujad analüüsivad, kas materjal on käesoleva määruse tähenduses terroristlik, peaksid nad arvesse võtma selliseid aspekte nagu avalduste laad ja sõnastus, avalduste tegemise kontekst ja tõenäosus, et neil on kahjulikud tagajärjed inimeste turvalisusele ja ohutusele. Oluline tegur, mida hindamisel arvesse võtta, peaks olema see, kui materjali on koostanud isik, rühmitus või üksus, kes on kantud terroriaktidega seotud isikute, rühmituste ja üksuste liidu loetellu ning kelle suhtes kohaldatakse piiravaid meetmeid, selle võib talle omistada või seda levitatakse tema nimel.

---

[1] Euroopa Parlamendi ja nõukogu 15. märtsi 2017. aasta direktiiv (EL) 2017/541 terrorismivastase võitluse kohta, millega asendatakse nõukogu raamotsus 2002/475/JSK ning muudetakse nõukogu otsust 2005/671/JSK (ELT L 88, 31.3.2017, lk 6).

(12) Materjali, mida levitatakse hariduslikul, ajakirjanduslikul, kunstilisel või teaduslikul eesmärgil või teadlikkuse suurendamiseks terroristliku tegevuse kohta ei tuleks pidada terroristlikuks sisuks. Selleks et määrata kindlaks, kas sisuteenuse pakkuja edastatud materjal kujutab endast „terroristlikku sisu“ käesoleva määruse tähenduses, tuleks arvesse võtta eelkõige väljendus- ja teabevabadust, sealhulgas meediavabadust ja meedia mitmekesisust, ning kunsti ja teaduse vabadust. Eriti juhtudel, kui sisuteenuse pakkujal on toimetusvastutus, tuleks levitatud materjali eemaldamise otsuse korral võtta arvesse ajakirjandusstandardeid, mis on kehtestatud ajakirjandus- või meediaalase reeglistikuga, kooskõlas liidu õiguse, sealhulgas hartaga. Terroristlikuks sisuks ei tohiks pidada radikaalsete, poleemiliste või vastuoluliste seisukohtade väljendamist tundlike poliitiliste küsimuste üle peetavas avalikus mõttevahetuses.

(13) Et terroristlikku veebisisu levitamise vastu tõhusalt võidelda, tagades samal ajal üksikisikute eraelu austamise, tuleks käesolevat määrust kohaldada infoühiskonna teenuste osutajate suhtes, kes teenuse kasutaja palvel talletavad ja levitavad üldsusele teavet ja materjali, mille teenuse kasutaja on esitanud, olenemata sellest, kas sellise teabe ja materjali talletamine ja üldsusele levitamine on pelgalt tehnilist, automaatset ja passiivset laadi. Mõiste „talletamine“ all tuleks mõista andmete hoidmist füüsilise või virtuaalse serveri mälus. Seetõttu peaks käesoleva määruse kohaldamisalast jääma välja „pelga edastamise“ või „vahemälu“ teenuste ja veebitaristu muudes kihtides muude teenuste pakkujad, kelle tegevus ei hõlma talletamist, näiteks registrid ja registripidajad, samuti domeeninimede süsteemide (DNS), makseteenuste ja hajusa teenusetõkestuse kaitse (DDoS) teenuste pakkujad.

(14) Mõiste „üldsusele levitamine“ peaks hõlmama teabe kättesaadavaks tegemist potentsiaalselt piiramatule arvule isikutele, tehes teabe kasutajatele üldiselt kergesti kättesaadavaks, ilma et sisuteenuse pakkujalt nõutaks edasisi meetmeid, olenemata sellest, kas need isikud kõnealuse teabega tegelikult tutvuvad. Seega, kui juurdepääs teabele eeldab registreerimist või kasutajarühma vastuvõtmist, tuleks seda teavet käsitada üldsusele levitatuna üksnes juhul, kui teabele juurdepääsu soovivad kasutajad registreeritakse või võetakse vastu automaatselt, ilma et keegi otsustaks või valiks, kellele juurdepääs võimaldada. Käesoleva määruse kohaldamisalasse ei peaks kuuluma isikutevahelise side teenused, nagu need on määratletud Euroopa Parlamendi ja nõukogu direktiivi (EL) 2018/1972 artikli 2 punktis 5[1], näiteks e-kirjad või privaatsõnumiteenused. Käesoleva määruse tähenduses tuleks lugeda teabe talletamiseks ja üldsusele levitamiseks üksnes tegevust, mis toimub sisuteenuse pakkuja otsese taotluse alusel. Seetõttu ei peaks käesolev määrus hõlmama näiteks selliste teenuste pakkujaid nagu pilveteenused, mida pakutakse muude isikute kui sisuteenuse pakkujate taotlusel ja millest viimased saavad üksnes kaudset kasu. Käesolev määrus peaks hõlmama sotsiaalmeedia, video-, pildi- ja audiomaterjalide jagamise teenuste ning failide jagamise teenuste ja muude pilveteenuste osutajaid niivõrd, kuivõrd neid teenuseid kasutatakse talletatud teabe üldsusele kättesaadavaks tegemiseks sisuteenuse pakkuja otsese taotluse alusel. Kui veebimajutusteenuse pakkuja pakub mitut teenust, tuleks käesolevat määrust kohaldada üksnes selle kohaldamisalasse kuuluvatele teenustele.

[1] Euroopa Parlamendi ja nõukogu 11. detsembri 2018. aasta direktiiv (EL) 2018/1972, millega kehtestatakse Euroopa elektroonilise side seadustik (ELT L 321, 17.12.2018, lk 36).

(15) Terroristlikku sisu levitatakse üldsusele sageli teenuste kaudu, mida osutavad veebimajutusteenuse pakkujad, kelle tegevuskoht on kolmandas riigis. Selleks et kaitsta liidu kasutajaid ja tagada, et kõigi digitaalsel ühtsel turul tegutsevate veebimajutusteenuse pakkujate suhtes kohaldatakse samu nõudeid, tuleks käesolevat määrust kohaldada kõigi liidus pakutavate asjakohaste teenuste osutajate suhtes, olenemata nende peamise tegevuskoha riigist. Veebimajutusteenuse pakkuja tuleks lugeda liidus teenuseid osutavaks kui ta võimaldab oma teenuseid kasutada füüsilistel või juriidilistel isikutel ühes või mitmes liikmesriigis ja kui tal on selle liikmesriigi või nende liikmesriikidega oluline seos.

(16) Oluline seos liiduga peaks olema olemas, kui veebimajutusteenuse pakkujal on liidus tegevuskoht, kui tema teenuseid kasutab märkimisväärne arv kasutajaid ühes või mitmes liikmesriigis või kui tema tegevus on suunatud ühte või mitmesse liikmesriiki. Tegevuse suunatuse ühte või mitmesse liikmesriiki peaks saama kindlaks teha kõigi asjakohaste asjaolude alusel, mille hulka kuuluvad sellised tegurid nagu asjaomases liikmesriigis üldiselt kasutatava keele või vääringu kasutamine või kaupade või teenuste tellimise võimalus asjaomasest liikmesriigist. Suunatust konkreetsesse liikmesriiki saab järeldada ka rakenduse kättesaadavuse alusel asjaomase liikmesriigi rakenduste poes, kohaliku reklaami või asjaomases liikmesriigis üldiselt kasutatavas keeles reklaami pakkumisest või kliendisuhete haldamisest, näiteks klienditeenuse pakkumisest asjaomases liikmesriigis üldiselt kasutatavas keeles. Olulise seose olemasolu tuleks eeldada ka juhul, kui veebimajutusteenuse pakkuja suunab oma tegevuse ühte või mitmesse liikmesriiki Euroopa Parlamendi ja nõukogu määruse (EL) nr 1215/2012[1] artikli 17 lõike 1 punkti c tähenduses. Üksnes asjaolu, et veebimajutusteenuse pakkuja veebisait, e-posti aadress või muud kontaktandmed on kättesaadavad ühes või mitmes liikmesriigis, ei peaks eraldivõetuna olema piisav, et kujutada endast olulist seost. Veelgi enam, kui teenust osutatakse ainult selleks, et järgida Euroopa Parlamendi ja nõukogu määruses (EL) 2018/302[2] sätestatud diskrimineerimiskeeldu, ei peaks üksnes selle alusel otsustama, et on olemas oluline seos liiduga.

---

[1] Euroopa Parlamendi ja nõukogu 12. detsembri 2012. aasta määrus (EL) nr 1215/2012 kohtualluvuse ning kohtuotsuste tunnustamise ja täitmise kohta tsiviil- ja kaubandusasjades (ELT L 351, 20.12.2012, lk 1).

[2] Euroopa Parlamendi ja nõukogu 28. veebruari 2018. aasta määrus (EL) 2018/302, mis käsitleb siseturul toimuvat põhjendamatut asukohapõhist tõkestust ja muul viisil diskrimineerimist kliendi kodakondsuse, elukoha või asukoha alusel ning millega muudetakse määrusi (EÜ) nr 2006/2004 ja (EL) 2017/2394 ning direktiivi 2009/22/EÜ (ELT L 60 I, 2.3.2018, lk 1).

(17) Ühtlustada tuleks menetlused ja kohustused, mis tulenevad eemaldamiskorraldusest, mille kohaselt peaks veebimajutusteenuse pakkuja eemaldama terroristliku sisu või blokeerima juurdepääsu sellele pärast pädeva asutuse hindamist. Arvestades, kui kiiresti levib terroristlik sisu veebiteenuste vahel, tuleks veebimajutusteenuse pakkujale panna kohustus tagada, et eemaldamiskorralduses kirjeldatud terroristlik sisu eemaldatakse või juurdepääs sellele blokeeritakse kõikides liikmesriikides ühe tunni jooksul alates eemaldamiskorralduse kättesaamisest. Välja arvatud kohaselt põhjendatud hädaolukordades peaks pädev asutus esitama veebimajutusteenuse pakkujale vähemalt 12 tundi enne talle esimese eemaldamiskorralduse tegemist teabe menetluste ja kohaldatavate tähtaegade kohta. Kohaselt põhjendatud hädaolukord on see, kui terroristliku sisu eemaldamine või sellele juurdepääsu blokeerimine hiljem kui ühe tunni möödumisel eemaldamiskorralduse kättesaamisest põhjustaks tõsist kahju, näiteks olukordades, kus on vahetu oht inimeste elule või kehalisele puutumatusele, või kui selline sisu mõjutaks sündmusi, mis kahjustavad inimeste elu või kehalist puutumatust. Pädev asutus peaks tegema kindlaks, kas juhtumi puhul on tegemist hädaolukorraga ja oma otsust eemaldamiskorralduses kohaselt põhjendama. Kui veebimajutusteenuse pakkuja ei saa eemaldamiskorraldust täita ühe tunni jooksul alates selle saamisest vääramatu jõu või objektiivse võimatuse tõttu, sealhulgas objektiivselt põhjendatud tehnilised või korralduslikud põhjused, peaks ta teavitama eemaldamiskorralduse teinud pädevat asutust nii kiiresti kui võimalik ja täitma eemaldamiskorralduse niipea, kui olukord on lahendatud.

(18) Eemaldamiskorraldus peaks sisaldama põhjendusi, mille alusel materjal, mis eemaldatakse või millele juurdepääs blokeeritakse, kvalifitseeritakse terroristlikuks sisuks, ning piisavat teavet võimaldamaks määrata kindlaks nimetatud sisu asukoht, esitades selleks täpse URLi ja vajaduse korral muu lisateabe, näiteks kuvatõmmise asjaomasest sisust. Põhjendused peaksid võimaldama veebimajutusteenuse pakkujal ja lõpuks sisuteenuse pakkujal kasutada tõhusalt oma õigust õiguskaitsele. Esitatud põhjendused ei tohiks kaasa tuua tundliku teabe avalikustamist, mis võiks käimasolevaid uurimisi kahjustada.

(19) Pädev asutus peaks esitama eemaldamiskorralduse otse kontaktpunktile, kelle veebimajutusteenuse pakkuja on käesoleva määruse kohaldamiseks määranud või asutanud, elektroonilisel kujul, mille kohta jääb kirjalik jälg, tingimustel, mis võimaldavad veebimajutusteenuse pakkujal teha kindlaks korralduse autentsuse, muu hulgas selle saatmise ja kättesaamise täpse kuupäeva ja kellaaja; selleks kasutatakse näiteks turvalisi e-kirju või platvorme või muid turvalisi kanaleid, mille hulka kuuluvad ka need, mille on teinud kättesaadavaks veebimajutusteenuse pakkuja, kooskõlas isikuandmete kaitset käsitleva liidu õigusega. Selle nõude täitmiseks peaks olema muu hulgas võimalik kasutada kvalifitseeritud e-andmevahetusteenuseid vastavalt Euroopa Parlamendi ja nõukogu määrusele (EL) nr 910/2014[1]. Kui veebimajutusteenuse pakkuja peamine tegevuskoht või tema seadusliku esindaja elu- või tegevuskoht on muus liikmesriigis kui eemaldamiskorralduse teinud pädev asutus, tuleks kõnealuse eemaldamiskorralduse koopia esitada samal ajal kõnealuse liikmesriigi pädevale asutusele.

[1] Euroopa Parlamendi ja nõukogu 23. juuli 2014. aasta määrus (EL) nr 910/2014 e-identimise ja e-tehingute jaoks vajalike usaldusteenuste kohta siseturul ja millega tunnistatakse kehtetuks direktiiv 1999/93/EÜ (ELT L 257, 28.8.2014, lk 73).

(20) Selle liikmesriigi pädeval asutusel, kus on veebimajutusteenuse pakkuja peamine tegevuskoht või tema seadusliku esindaja elu- või tegevuskoht, peaks olema võimalik kontrollida teise liikmesriigi pädevate asutuste tehtud eemaldamiskorraldust, et teha kindlaks, kas see rikub tõsiselt või ilmselt käesolevat määrust või hartas sätestatud põhiõigusi. Nii sisuteenuse pakkujal kui ka veebimajutusteenuse pakkujal peaks olema õigus taotleda kontrolli selle liikmesriigi pädevalt asutuselt, kus on veebimajutusteenuse pakkuja peamine tegevuskoht või tema seadusliku esindaja elu- või tegevuskoht. Kui selline taotlus esitatakse, peaks nimetatud pädev asutus võtma vastu otsuse, kas eemaldamiskorraldus sisaldab selliseid rikkumisi. Kui selles otsuses leitakse, et selline rikkumine esineb, tuleks eemaldamiskorralduse õiguslikud tagajärjed tühistada. Kontroll tuleks teha kiiresti, et tagada ekslikult eemaldatud sisu või sellele juurdepääsu võimalikult kiire taastamine.

(21) Terroristliku sisuga kokku puutuvad veebimajutusteenuse pakkujad peaksid lisama nende olemasolul oma teenuse kasutamise tingimustesse klausli, mis käsitleb nende teenuste kuritarvitamist terroristliku veebisisu levitamiseks. Nad peaksid seda klauslit kohaldama hoolikalt, läbipaistvalt, proportsionaalselt ja mittediskrimineerivalt.

(22) Arvestades probleemi ulatust ja kiirust, millega on vaja tegutseda, et terroristlik sisu tõhusalt kindlaks teha ja eemaldada, on tõhusad ja proportsionaalsed erimeetmed terroristliku veebisisu vastu võitlemises olulisel kohal. Et vähendada terroristlikule sisule juurdepääsetavust oma teenuste kaudu, peaksid terroristliku sisuga kokku puutunud veebimajutusteenuse pakkujad võtma erimeetmeid, võttes arvesse terroristliku sisuga kokkupuutumise riske ja ulatust ning seda, millist mõju see avaldab kolmandate isikute õigustele ja üldsuse huvile olla informeeritud. Veebimajutusteenuse pakkujad peaksid kindlaks määrama, milline asjakohane, tõhus ja proportsionaalne erimeede tuleks kehtestada terroristliku sisu kindlakstegemiseks ja eemaldamiseks. Erimeetmed võivad hõlmata asjakohaseid tehnilisi või korralduslikke meetmeid või suutlikkust, näiteks personali või tehnilisi vahendeid terroristliku sisu kindlakstegemiseks ja kiireks eemaldamiseks või sellele juurdepääsu blokeerimiseks, mehhanisme, mis võimaldavad kasutajatel teatada väidetavast terroristlikust sisust või see märgistada, või muid meetmeid, mida veebimajutusteenuse pakkuja peab asjakohaseks ja tõhusaks, et võidelda terroristliku sisu kättesaadavuse vastu oma teenuste kaudu.

(23) Erimeetmete kehtestamisel peaks veebimajutusteenuse pakkuja tagama, et säilib harta alusel kaitstav kasutajate õigus väljendus- ja teabevabadusele, samuti meediavabadus ja meedia mitmekesisus. Lisaks selliste õigusest tulenevate nõuete järgimisele, mis on ette nähtud muu hulgas isikuandmete kaitset käsitletavate õigusaktidega, peaksid veebimajutusteenuse pakkujad tegutsema nõuetekohase hoolsusega ja rakendama asjakohasel juhul kaitsemeetmeid, sealhulgas inimeste tehtavat jälgimist ja kontrollimist, et vältida tahtmatuid või ekslikke otsuseid, mille tulemusena eemaldataks sisu, mis ei ole terroristlik, või blokeeritaks sellele juurdepääs.

(24) Veebimajutusteenuse pakkuja peaks teatama pädevale asutusele kehtestatud erimeetmetest, et nimetatud asutus saaks otsustada, kas meetmed on tõhusad ja proportsionaalsed ning juhul, kui kasutatakse automaatseid vahendeid, ka selle, kas veebimajutusteenuse pakkujal on inimeste tehtava jälgimise ja kontrollimise suutlikkus. Meetmete tõhususe ja proportsionaalsuse hindamisel peaksid pädevad asutused võtma arvesse asjaomaseid parameetreid, sealhulgas veebimajutusteenuse pakkujale tehtud eemaldamiskorralduste arvu, veebimajutusteenuse pakkuja suurust ja majanduslikku suutlikkust ja tema teenuste mõju terroristliku sisu levitamisele, näiteks kasutajate arvu alusel liidus, samuti kaitsemeetmeid, mis on kehtestatud, et võidelda nende teenuste kuritarvitamise vastu terroristliku veebisisu levitamiseks.

(25) Kui pädev asutus leiab, et kehtestatud erimeetmed ei ole riskidega tegelemiseks piisavad, peaks tal olema võimalik nõuda täiendavate asjakohaste, tõhusate ja proportsionaalsete erimeetmete võtmist. Selliste täiendavate erimeetmete rakendamise nõue ei tohiks kaasa tuua üldist seirekohustust ega faktide otsimise kohustust direktiivi 2000/31/EÜ artikli 15 lõike 1 tähenduses, ega automaatsete vahendite kasutamise kohustust. Veebimajutusteenuse pakkujatel peaks siiski olema võimalik otsustada kasutada automaatseid vahendeid, kui nad peavad seda asjakohaseks ja vajalikuks, et tõhusalt võidelda oma teenuste kuritarvitamise vastu terroristliku veebisisu levitamiseks.

(26) Veebimajutusteenuse pakkuja kohustus säilitada eemaldatud sisu ja sellega seotud andmed tuleks kehtestada kindlal eesmärgil ja üksnes nii kauaks kui vaja. Säilitamisnõue peab laienema seotud andmetele, sest vastasel juhul läheksid sellised andmed kõnealuse terroristliku sisu eemaldamise tagajärjel kaotsi. Seotud andmed võivad olla kliendi andmed, eeskätt andmed sisuteenuse pakkuja identiteedi kohta, samuti juurdepääsuandmed, kaasa arvatud andmed kuupäeva ja kellaaja kohta, millal sisuteenuse pakkuja teenust kasutas, ja teenusesse sisse ja sealt välja logimise kohta, ning IP-aadress, mille veebiühenduse pakkuja on sisuteenuse pakkujale eraldanud.

(27) Kohustus säilitada sisu halduslikus või kohtulikus korras toimuva läbivaatamismenetluse jaoks on vajalik ja põhjendatud vajadusega tagada tulemuslikud õiguskaitsevahendid sisuteenuse pakkujale, kelle sisu eemaldati või kelle sisule juurdepääs blokeeriti, ning tagada selle sisu taastamine vastavalt nende menetluste tulemustele. Kohustus säilitada materjale uurimise või süüdistuse esitamisega seotud eesmärgil on põhjendatud ja vajalik, arvestades kõnealuse materjali väärtust terrorismi nurjamisel ja tõkestamisel. Seepärast tuleks lugeda põhjendatuks ka eemaldatud terroristliku sisu säilitamist terroriaktide tõkestamise, avastamise, uurimise ja nende eest süüdistuse esitamise eesmärgil. Terroristlikku sisu ja sellega seotud andmeid tuleks talletada üksnes ajavahemiku jooksul, mida on vaja, et õiguskaitseasutused saaksid seda terroristlikku sisu kontrollida ja otsustada, kas see on nimetatud eesmärkidel vajalik. Terroriaktide tõkestamise, avastamise, uurimise ja nende eest süüdistuse esitamise eesmärgil andmete säilitamise nõue peaks piirduma andmetega, millel on tõenäoliselt seos terroriaktidega ja mis võivad seega aidata esitada süüdistust terroriakti eest või hoida ära tõsiseid avalikku julgeolekut ohustavaid riske. Kui veebimajutusteenuse pakkuja eemaldab materjali või blokeerib sellele juurdepääsu, eeskätt oma erimeetmete abil, peaks ta teavitama pädevaid asutusi viivitamata sisust, mis sisaldab teavet, millega kaasneb või millest lähtub vahetu oht elule või terroriakti kahtlus.

(28) Proportsionaalsuse tagamise huvides tuleks andmete säilitamise ajaks määrata kuni kuus kuud, et sisuteenuse pakkujale jääks piisavalt aega, et algatada halduslik või kohtulik läbivaatamismenetlus ja anda õiguskaitseasutustele juurdepääs terroriaktide uurimise ja nende eest süüdistuse esitamise seisukohast olulistele andmetele. Kui need menetlused algatatakse, kuid neid ei viida kuue kuu jooksul lõpuni, peaks pädeva asutuse või kohtu taotlusel olema võimalik seda ajavahemikku pikendada nii kauaks kui vaja. Andmete säilitamise aeg peaks olema piisav, et õiguskaitseasutused saaksid uurimistega ja süüdistuste esitamisega seotud vajalikud materjalid säilitada, tagades ühtlasi tasakaalu põhiõigustega.

(29) Käesolev määrus ei tohiks mõjutada menetluslikke tagatisi või uurimismeetmeid, mis on seotud juurdepääsuga sisule ja seotud andmetele, mida säilitatakse terroriaktide uurimise ja nende eest süüdistuse esitamise eesmärgil vastavalt liidu või liikmesriikide õigusele.

(30) Veebimajutusteenuse pakkujate terroristlikku sisu käsitlevate põhimõtete läbipaistvus on äärmiselt tähtis, et suurendada nende vastutust kasutajate ees ja kodanike usaldust digitaalse ühtse turu vastu. Veebimajutusteenuse pakkujad, kes on asjaomasel kalendriaastal võtnud terroristliku sisu levitamise vastu meetmeid või kellelt on nõutud meetmete võtmist vastavalt käesolevale määrusele, peaksid igal aastal tegema üldsusele kättesaadavaks läbipaistvusaruande, mis sisaldab teavet terroristliku sisu kindlakstegemiseks ja eemaldamiseks võetud meetmete kohta.

(31) Pädevad asutused peaksid igal aastal avaldama läbipaistvusaruanded, mis sisaldavad teavet eemaldamiskorralduste arvu, selliste juhtumite arvu, kui määrust ei täidetud, erimeetmeid käsitlevate otsuste arvu, haldusliku või kohtuliku läbivaatamismenetluse alla kuuvate juhtumite arvu ning karistusi määravate otsuste arvu kohta.

(32) Euroopa Liidu lepingu (ELi leping) artiklis 19 ja harta artiklis 47 on selgelt kirjas õigus tõhusale õiguskaitsevahendile. Igal füüsilisel ja juriidilisel isikul on õigus pöörduda liikmesriigi pädeva kohtu poole tõhusa õiguskaitsevahendi saamiseks kõigi käesoleva määruse kohaselt võetud meetmete vastu, mis võivad selle isiku õigusi kahjustada. Eeskätt peaks see õigus hõlmama veebimajutusteenuse ja sisuteenuse pakkujate jaoks võimalust vaidlustada eemaldamiskorraldus või otsus, mis tuleneb eemaldamiskorralduse kontrollimisest vastavalt käesolevale määrusele, selle liikmesriigi kohtus, kelle pädev asutus eemaldamiskorralduse tegi või otsuse vastu võttis, ning veebimajutusteenuse pakkujate jaoks võimalust vaidlustada erimeetmeid või karistusi käsitlev otsus selle liikmesriigi kohtus, kelle pädev asutus kõnealuse otsuse vastu võttis.

(33) Kaebuste lahendamise menetlused on vajalik kaitsemeede veebisisu eksliku eemaldamise või sellele juurdepääsu blokeerimise eest, kui selline sisu on kaitstud väljendus- ja teabevabaduse alusel. Seepärast peaksid veebimajutusteenuse pakkujad sisse seadma kasutajasõbralikud kaebuste esitamise mehhanismid ja tagama, et kaebustega tegeletakse kiiresti ja sisuteenuse pakkuja seisukohast täiesti läbipaistvalt. Kohustus, et veebimajutusteenuse pakkuja peab taastama ekslikult eemaldatud sisu või sisu, millele juurdepääs blokeeriti, ei mõjuta veebimajutusteenuse pakkuja võimalust tagada oma tingimuste täitmine muudel alustel.

(34) Tõhus õiguskaitse, mis on kooskõlas ELi lepingu artikliga 19 ja harta artikliga 47, eeldab, et sisuteenuse pakkujad saavad tutvuda põhjendustega, mille alusel nende pakutav sisu on eemaldatud või juurdepääs sellele blokeeritud. Sellel eesmärgil peaks veebimajutusteenuse pakkuja tegema sisuteenuse pakkujale kättesaadavaks teabe, et sisuteenuse pakkujal oleks võimalik vaidlustada sisu eemaldamise või sellele juurdepääsu blokeerimise otsus. Olenevalt asjaoludest võib majutusteenuse pakkuja asendada eemaldatud sisu või sisu, millele juurdepääs on blokeeritud, sõnumiga selle kohta, et sisu on eemaldatud või juurdepääs sellele blokeeritud kooskõlas käesoleva määrusega. Sisuteenuse pakkuja taotluse korral tuleks anda lisateavet põhjuste kohta, miks sisu eemaldati või sellele juurdepääs blokeeriti, aga ka õiguskaitsevahendite kohta, mille abil eemaldamine või blokeerimine vaidlustada. Kui pädevad asutused otsustavad, et avaliku julgeolekuga seotud põhjustel, sealhulgas seoses uurimisega, oleks sisu eemaldamise või sellele juurdepääsu blokeerimise kohta käiva teabe esitamine otse sisuteenuse pakkujale sobimatu või kahjulik, peaksid nad teavitama veebimajutusteenuse pakkujat.

(35) Liikmesriigid peaksid määrama käesoleva määruse kohaldamiseks pädevad asutused. See ei peaks tingimata eeldama uue asutuse loomist ja käesolevas määruses sätestatud ülesanded peaks olema võimalik anda olemasolevale asutusele. Käesoleva määrusega tuleks nõuda asutuse määramist, kes oleks pädev tegema eemaldamiskorraldusi, kontrollima eemaldamiskorraldusi ning jälgima erimeetmeid ja määrama karistusi, jättes samas igale liikmesriigile võimaluse ise otsustada, mitu pädevat asutust nad määravad ja kas need on haldus-, õiguskaitse- või kohtuasutused. Liikmesriigid peaksid tagama, et pädev asutus täidab oma ülesandeid objektiivselt ja mittediskrimineerivalt ning ei küsi ega võta vastu juhiseid üheltki teiselt organilt seoses käesoleva määruse kohaste ülesannete täitmisega. See ei peaks välistama liikmesriigi õiguse kohast järelevalvet. Liikmesriigid peaksid teavitama käesoleva määruse kohaselt määratud pädevatest asutustest komisjoni, kes peaks veebis avaldama pädevate asutuste registri. Veebiregister peaks olema hõlpsasti kättesaadav, et veebimajutusteenuse pakkujatel oleks lihtne eemaldamiskorralduste ehtsust kiiresti kontrollida.

(36) Enne kui pädevad asutused teevad eemaldamiskorralduse, peaksid nad jagama teavet, koordineerima ja tegema koostööd omavahel ja asjakohasel juhul ka Europoliga, et vältida topelttööd ja võimalikku sekkumist uurimistesse ning minimeerida mõjutatud veebimajutusteenuse pakkuja koormust. Eemaldamiskorralduse tegemise üle otsustades peaks pädev asutus võtma kohaselt arvesse teateid uurimistesse sekkumiste kohta (dekonfliktimine). Kui ühe liikmesriigi pädev asutus teavitab teise liikmesriigi pädevat asutust kehtivast eemaldamiskorraldusest, ei peaks teise liikmesriigi pädev asutus sama asja kohta eemaldamiskorraldust tegema. Käesoleva määruse sätete rakendamisel võiks Europol pakkuda toetust kooskõlas oma praeguste volituste ja kehtiva õigusraamistikuga.

(37) Veebimajutusteenuse pakkujate võetud erimeetmete tulemusliku ja piisavalt sidusa rakendamise tagamiseks peaksid pädevad asutused koordineerima ja tegema üksteisega koostööd seoses teabevahetusega veebimajutusteenuse pakkujatega eemaldamiskorralduste ja erimeetmete kindlaksmääramise, rakendamise ja hindamise osas. Koordineerimine ja koostöö on vajalik ka teiste käesoleva määruse rakendamismeetmete puhul sealhulgas seoses karistusi käsitlevate normide vastuvõtmise ning karistuste määramisega. Komisjon peaks sellist koordineerimist ja koostööd hõlbustama.

(38) On äärmiselt oluline, et karistuste kehtestamise eest vastutava liikmesriigi pädev asutus oleks täielikult teadlik eemaldamiskorralduste tegemisest ja sellele järgnevast teabevahetusest veebimajutusteenuse pakkuja ja teiste liikmesriikide pädevate asutuste vahel. Selleks peaksid liikmesriigid tagama asjakohaste ja turvaliste sidekanalite ja -mehhanismide olemasolu, mille kaudu saaks asjakohast teavet õigeaegselt jagada.

(39) Sujuva teabevahetuse hõlbustamiseks pädevate asutuste vahel ja ka veebimajutusteenuse pakkujatega ning topelttöö vältimiseks peaks julgustama liikmesriike kasutama Europoli välja töötatud asjaomaseid vahendeid, näiteks praegu kasutusel olevat veebisisust teavitamise haldamise rakendust või tulevasi rakendusi.

(40) Liikmesriikide ja Europoli esildised on osutunud tõhusaks ja kiireks vahendiks, et suurendada veebimajutusteenuse pakkujate teadlikkust nende teenuste kaudu kättesaadavast konkreetsest sisust ja võimaldada neil kiiresti tegutseda. Need esildised, mis on mehhanism, millega saab juhtida veebimajutusteenuse pakkuja tähelepanu teabele, mida võib pidada terroristlikuks sisuks, et teenusepakkuja saaks vabatahtlikult kaaluda selle sisu vastavust oma tingimustele, peaksid eemaldamiskorralduste kõrval kasutusele jääma. Lõpliku otsuse selle kohta, kas teave eemaldada tingimustele mittevastavuse tõttu, teeb veebimajutusteenuse pakkuja. Käesolev määrus ei peaks mõjutama Euroopa Parlamendi ja nõukogu määruses (EL) 2016/7941[1] sätestatud Europoli volitusi. Seetõttu ei tohiks ühtki käesoleva määruse sätet tõlgendada nii, et see takistaks liikmesriike ja Europoli kasutamast esildisi terroristliku veebisisu vastu võitlemise vahendina.

[1] Euroopa Parlamendi ja nõukogu 11. mai 2016. aasta määrus (EL) 2016/794, mis käsitleb Euroopa Liidu Õiguskaitsekoostöö Ametit (Europol) ning millega asendatakse ja tunnistatakse kehtetuks nõukogu otsused 2009/371/JSK, 2009/934/JSK, 2009/935/JSK, 2009/936/JSK ja 2009/968/JSK (ELT L 135, 24.5.2016, lk 53).

(41) Arvestades, et teatava terroristliku veebisisu tagajärjed võivad olla eriti tõsised, peaks veebimajutusteenuse pakkuja viivitamata teavitama asjaomase liikmesriigi ametiasutusi või selle liikmesriigi pädevaid asutusi, kus on ta tegevuskoht või kus tal on seaduslik esindaja, terroristlikust sisust, millega kaasneb või millest lähtub vahetu oht elule või terroriakti kahtlus. Proportsionaalsuse tagamise huvides peaks see kohustus kehtima vaid selliste terroriaktide puhul, mis on määratletud direktiivi (EL) 2017/541 artikli 3 lõikes 1. Teavitamiskohustus ei tähenda, et veebimajutusteenuse pakkujatel oleks kohustus otsida aktiivselt tõendeid sellise vahetu ohu kohta elule või terroriakti kahtluse kohta. Asjaomase liikmesriigina tuleks mõista on liikmesriiki, kelle jurisdiktsiooni alla terroriaktide uurimine ja nende eest süüdistuse esitamine kuulub, lähtudes õigusrikkuja või õigusrikkumise võimaliku ohvri kodakondsusest või terroriakti sihtkohast. Kahtluse korral peaks veebimajutusteenuse pakkuja esitama teabe Europolile, kes peaks võtma asjakohaseid edasisi meetmeid vastavalt oma volitustele ning muu hulgas edastama selle teabe liikmesriikide asjaomastele ametiasutustele. Liikmesriikide pädevatel asutustel peaks olema lubatud kasutada sellist teavet liidu või liikmesriigi õiguse kohaste uurimistoimingute jaoks .

(42) Veebimajutusteenuse pakkujad peaksid määrama või looma kontaktpunktid, et hõlbustada eemaldamiskorralduste kiiret menetlemist. Kontaktpunkt peaks täitma üksnes korralduslikke eesmärke. Kontaktpunkti peaksid moodustama sihtotstarbelised asutusesisesed või lepingulised vahendid, mille abil saab elektrooniliselt esitada eemaldamiskorraldusi, ning nende kiireks töötlemiseks vajalikud tehnilised vahendid või inimressursid. Kontaktpunkt ei pea asuma liidus. Veebimajutusteenuse pakkujal peaks olema vabadus nimetada käesoleva määruse täitmiseks mõni olemasolev kontaktpunkt, kui see kontaktpunkt suudab täita käesolevas määruses sätestatud ülesandeid. Selleks et terroristlik sisu eemaldataks või juurdepääs sellele blokeeritaks ühe tunni jooksul pärast eemaldamiskorralduse saamist, peaksid terroristliku sisuga kokku puutunud veebimajutusteenuse pakkuja kontaktpunktid olema kogu aeg kättesaadavad. Teave kontaktpunkti kohta peaks sisaldama teavet selle kohta, mis keeles saab kontaktpunkti poole pöörduda. Hõlbustamaks teabevahetust veebimajutusteenuse pakkujate ja pädevate asutuste vahel, kutsutakse veebimajutusteenuse pakkujaid üles võimaldama suhtlust ühes liidu institutsioonide ametlikest keeltest, milles on kättesaadavad nende teenuse tingimused.

(43) Kuna puudub üldine nõue, et veebimajutusteenuse pakkujad peavad tagama füüsilise kohalviibimise liidu territooriumil, on vaja tagada selgus selle kohta, millise liikmesriigi jurisdiktsiooni alla liidus teenuseid pakkuv veebimajutusteenuse pakkuja kuulub. Üldiselt kuulub veebimajutusteenuse pakkuja selle liikmesriigi jurisdiktsiooni alla, kus on tema peamine tegevuskoht või kus on tema seadusliku esindaja elu- või tegevuskoht. See ei tohiks piirata selliste pädevust käsitlevate normide kohaldamist, mis on kehtestatud eemaldamiskorralduste ja eemaldamiskorralduse kontrollimisest tulenevate otsuste jaoks vastavalt käesolevale määrusele. Veebimajutusteenuse pakkuja üle, kellel puudub liidus tegevuskoht ja kes ei määra endale seaduslikku esindajat, peaks kõik liikmesriigid saama teostada jurisdiktsiooni ja seega peaks kõigil liikmesriikidel olema võimalus määrata talle karistusi tingimusel, et järgitakse topeltkaristamise keeldu.

(44) Veebimajutusteenuse pakkuja, kelle tegevuskoht ei ole liidus, peaks määrama kirjalikus vormis seadusliku esindaja, et tagada käesoleva määruse järgimine ja sellest tulenevate kohustuste täitmine. Veebimajutusteenuse pakkujal peaks olema võimalik määrata käeoleva määruse kohaldamiseks seaduslik esindaja, kelle ta on juba muul otstarbel määranud, tingimusel, et kõnealune esindaja suudab täita käesolevas määruses sätestatud funktsioone. Seaduslik esindaja peaks olema volitatud tegutsema veebimajutusteenuse pakkuja nimel.

(45) Karistused on vajalikud, et tagada käesoleva määruse tõhus rakendamine veebimajutusteenuse pakkuja poolt. Liikmesriigid peaksid kehtestama õigusnormid karistuste kohta, mis võivad olla haldus- või kriminaalkaristused, ning asjakohasel juhul trahvimise suunised. Kui nõudeid rikutakse üksikjuhtudel, võiks nende eest karistada, järgides topeltkaristamise keeldu ja proportsionaalsuse põhimõtet ning tagades, et selliste karistuste puhul võetakse arvesse süstemaatilist korralduste täitmata jätmist. Karistused võiksid olla eri vormis, sealhulgas ametlikud hoiatused väiksemate rikkumiste eest või rahalised karistused raskemate või süstemaatiliste rikkumiste eest. Eriti ranged karistused tuleks määrata juhul, kui veebimajutusteenuse pakkuja jätab terroristliku sisu süstemaatiliselt või korduvalt eemaldamata või süstemaatiliselt või korduvalt ei blokeeri juurdepääsu sellele ühe tunni jooksul pärast eemaldamiskorralduse kättesaamist. Õiguskindluse tagamiseks tuleks käesolevas määruses sätestada, milliste rikkumiste eest määratakse karistus ning milliseid asjaolusid võetakse karistuse liigi ja määra hindamisel arvesse. Rahalise karistuse määramise üle otsustamisel tuleks kohaselt arvesse võtta veebimajutusteenuse pakkuja rahalisi vahendeid. Lisaks peaks pädev asutus võtma arvesse, kas veebimajutusteenuse pakkuja on idufirma või mikro-, väike või keskmise suurusega ettevõtja nagu on määratletud komisjoni soovituses 2003/361/EÜ[1]. Arvesse tuleks võtta ka täiendavaid asjaolusid, näiteks seda, kas veebimajutusteenuse pakkuja käitumine on olnud objektiivselt ettevaatamatu või laiduväärne või kas rikkumine pandi toime hooletusest või tahtlikult. Liikmesriigid peaksid tagama, et käesoleva määruse rikkumise eest määratud karistused ei ärgitaks eemaldama materjali, mis ei ole terroristlik sisu.

[1] Komisjoni 6. mai 2003. aasta soovitus 2003/361/EÜ mikro-, väikeste ja keskmise suurusega ettevõtete määratlemise kohta (ELT L 124, 20.5.2003, lk 36).

(46) Standardvormide kasutamine hõlbustab koostööd ja teabevahetust pädevate asutuste ja veebimajutusteenuse pakkujate vahel ning võimaldab neil suhelda kiiremini ja tulemuslikumalt. Eriti oluline on tagada kiire tegutsemine pärast eemaldamiskorralduse kättesaamist. Vormide kasutamine vähendab tõlkekulusid ja edendab menetluse kvaliteeti. Tagasiside vormide kasutamine võimaldab standarditud teabevahetust ning need on eriti olulised olukorras, kui veebimajutusteenuse pakkuja ei suuda eemaldamiskorralduse nõudeid täita. Autenditud edastuskanalid saavad tagada eemaldamiskorralduse autentsuse, muu hulgas korralduse saatmise ja vastuvõtmise kuupäeva ja kellaaja täpsuse.

(47) Et käesoleva määruse kohaldamisel kasutatavate vormide sisu saaks vajaduse korral sujuvalt muuta, peaks komisjonil olema õigus võtta kooskõlas Euroopa Liidu toimimise lepingu artikli 290 vastu delegeeritud õigusakte käesoleva määruse lisade muutmiseks. Et oleks võimalik võtta arvesse tehnika ja asjaomase õigusraamistiku arengut, peaks komisjonil samuti olema õigus võtta vastu delegeeritud õigusakte, et täiendada käesolevat määrust tehniliste nõuetega elektrooniliste vahendite kohta, mida pädevad asutused peavad kasutama eemaldamiskorralduste edastamiseks. On eriti oluline, et komisjon viiks oma ettevalmistava töö käigus läbi asjakohaseid konsultatsioone, sealhulgas ekspertide tasandil, ja et kõnealused konsultatsioonid viidaks läbi kooskõlas 13. aprilli 2016. aasta institutsioonidevahelises parema õigusloome kokkuleppes[1] sätestatud põhimõtetega. Eelkõige selleks, et tagada delegeeritud õigusaktide ettevalmistamises võrdne osalemine, saavad Euroopa Parlament ja nõukogu kõik dokumendid liikmesriikide ekspertidega samal ajal ning nende ekspertidel on pidev juurdepääs komisjoni eksperdirühmade koosolekutele, millel arutatakse delegeeritud õigusaktide ettevalmistamist.

(48) Liikmesriigid peaksid koguma teavet käesoleva määruse rakendamise kohta. Liikmesriikidel peaks olema võimalik kasutada veebimajutusteenuse pakkujate läbipaistvusaruandeid ja esitada vajaduse korral täienduseks üksikasjalikumat teavet, näiteks käesoleva määruse kohaseid omapoolseid läbipaistvusaruandeid. Käesoleva määruse väljundite, tulemuste ja mõju seireks tuleks koostada üksikasjalik programm, millest lähtudes käesoleva määruse rakendamist hinnata.

[1] ELT L 123, 12.5.2016, lk 1.

(49) Komisjon peaks hindama käesolevat määrust kolme aasta jooksul alates selle jõustumise kuupäevast, lähtudes rakendamisaruande tähelepanekutest ja järeldustest ning seire tulemustest. Hindamisel tuleks lähtuda tõhususe, vajalikkuse, mõjususe, proportsionaalsuse, asjakohasuse, sidususe ja liidu lisaväärtuse kriteeriumidest. Hinnata tuleks mitmesuguste määruse kohaselt ette nähtud korralduslike ja tehniliste meetmete toimimist, sealhulgas selliste meetmete mõjusust, mille eesmärk on parandada terroristliku veebisisu avastamist, kindlakstegemist ja eemaldamist, kaitsemehhanismide mõjusust ning võimalikku mõju põhiõigustele nagu näiteks väljendus- ja teabevabadusele, sealhulgas meediavabadusele ja meedia mitmekesisusele, ettevõtlusvabadusele ning eraelu puutumatuse ja isikuandmete kaitse õigusele. Komisjon peaks hindama ka võimalikku mõju kolmandate isikute huvidele.

(50) Kuna käesoleva määruse eesmärki, nimelt tagada digitaalse ühtse turu sujuv toimimine terroristliku veebisisu levitamise vastu võitlemisega, ei suuda liikmesriigid piisavalt saavutada, küll aga saab seda meetme ulatuse ja mõju tõttu paremini saavutada liidu tasandil, võib liit võtta meetmeid kooskõlas ELi lepingu artiklis 5 sätestatud subsidiaarsuse põhimõttega. Kõnealuses artiklis sätestatud proportsionaalsuse põhimõtte kohaselt ei lähe käesolev määrus nimetatud eesmärgi saavutamiseks vajalikust kaugemale,

ON VASTU VÕTNUD KÄESOLEVA MÄÄRUSE:

I Jagu

Üldsätted

Artikkel 1

Reguleerimisese ja kohaldamisala

1. Käesolevas määruses nähakse ette ühtsed normid, et võidelda veebimajutusteenuste kuritarvitamise vastu terroristliku veebisisu levitamiseks üldsusele, eelkõige järgmise kohta:

   a) veebimajutusteenuse pakkujate mõistlik ja proportsionaalne hoolsuskohustus, et võidelda terroristliku sisu levitamise vastu üldsusele oma teenuste kaudu ja tagada vajaduse korral sellise sisu kiire eemaldamine või sellele juurdepääsu blokeerimine;

   b) meetmed, mille liikmesriigid peavad kehtestama kooskõlas liidu õigusega ja võttes asjakohaseid kaitsemeetmeid, et kaitsta põhiõigusi, eelkõige väljendus- ja teabevabadust avatud ja demokraatlikus ühiskonnas, et

      i) teha kindlaks terroristlik sisu ja tagada selle kiire eemaldamine veebimajutusteenuste pakkujate poolt ning

      ii) hõlbustada koostööd liikmesriikide pädevate asutuste, veebimajutusteenuste pakkujate ja asjakohasel juhul Europoliga.

2. Käesolevat määrust kohaldatakse liidus teenuseid pakkuvate veebimajutusteenuse pakkujate suhtes, kes levitavad üldsusele teavet, olenemata sellest, kus on nende peamine tegevuskoht.

3. Üldsusele hariduslikul, ajakirjanduslikul, kunstilisel või teaduslikul eesmärgil või terrorismi ennetamise või selle vastu võitlemise eesmärgil materjali levitamist, sealhulgas materjal, milles väljendatakse poleemilisi või vastuolulisi seisukohti avalikus mõttevahetuses, ei loeta terroristlikuks sisuks. Hindamisega määratakse kindlaks levitamise tegelik eesmärk ja kas materjali levitatakse üldsusele nimetatud eesmärkidel.

4. Käesolev määrus ei mõjuta kohustust austada õigusi, vabadusi ja põhimõtteid, millele on osutatud ELi lepingu artiklis 6, ning seda kohaldatakse piiramata väljendus- ja teabevabadust käsitlevaid põhimõtteid, sealhulgas meediavabadust ja meedia mitmekesisust.

5. Käesoleva määruse kohaldamine ei piira direktiivide 2000/31/EÜ ja 2010/13/EL kohaldamist. Direktiivi 2010/13/EL artikli 1 lõike 1 punktis a määratletud audiovisuaalmeedia teenuste puhul on ülimuslik direktiiv 2010/13/EL.

Artikkel 2

Mõisted

Käesolevas määruses kasutatakse järgmisi mõisteid:

1) „veebimajutusteenuse pakkuja“ – isik, kes pakub Euroopa Parlamendi ja nõukogu direktiivi (EL) 2015/1535[1] artikli 1 punktis b määratletud teenuseid, mis seisnevad sisuteenuse pakkuja antud teabe talletamises sisuteenuse pakkuja soovil;

2) „sisuteenuse pakkuja“ – kasutaja, kes on andnud teabe, mida veebimajutusteenuse pakkuja talletab ja üldsusele levitab või on talletanud ja üldsusele levitanud;

3) „üldsusele levitamine“ – teabe kättesaadavaks tegemine sisuteenuse pakkuja taotlusel potentsiaalselt piiramatule arvule isikutele;

4) „teenuste pakkumine liidus“ – võimaluse andmine ühe või mitme liikmesriigi füüsilistele või juriidilistele isikutele kasutada sellise veebimajutusteenuse pakkuja teenuseid, kellel on selle liikmesriigi või nende liikmesriikidega oluline seos;

[1] Euroopa Parlamendi ja nõukogu 9. septembri 2015. aasta direktiiv 2015/1535/EÜ, millega nähakse ette tehnilistest eeskirjadest ning infoühiskonna teenuste eeskirjadest teatamise kord (ELT L 241, 17.9.2015, lk 1).

5) „oluline seos“ – veebimajutusteenuse pakkuja seos ühe või mitme liikmesriigiga, mis tuleneb sellest, et tema tegevuskoht on liidus, või erilistest faktilistest kriteeriumidest nagu:

   a) ühes või mitmes liikmesriigis on märkimisväärne arv tema teenuste kasutajaid või

   b) veebimajutusteenuse pakkuja tegevus on suunatud ühele või mitmele liikmesriigile;

6) „terroriakt“ – direktiivi (EL) 2017/541 artiklis 3 määratletud kuritegu;

7) „terroristlik sisu“ – ühte või mitut järgmist liiki materjal, täpsemini materjal, mis:

   a) õhutab ühe direktiivi (EL) 2017/541 artikli 3 lõike 1 punktides a–i osutatud kuriteo toimepanemisele, kui selline materjal otseselt või kaudselt, näiteks terroriaktide ülistamisega, õigustab terroriaktide sooritamist, põhjustades seeläbi ohu, et võidakse toime panna üks või mitu sellist akti;

   b) ärgitab isikut või isikute rühma toime panema mõnda direktiivi (EL) 2017/541 artikli 3 lõike 1 punktides a–i loetletud kuritegu või sellele kaasa aitama;

c) ärgitab isikut või isikute rühma osalema terrorirühmituse tegevuses direktiivi (EL) 2017/541 artikli 4 punkti b tähenduses;

d) annab juhiseid lõhkeainete, tuli- või muude relvade või mürgiste või ohtlike ainete valmistamise või kasutamise kohta või muude konkreetsete meetodite või tehniliste võtete kohta, et toime panna mõni direktiivi (EL) 2017/541 artikli 3 lõike 1 punktides a–i osutatud terroriakt või selle toimepanemisele kaasa aidata;

e) kujutab ohtu seoses mõne direktiivi (EL) 2017/541 artikli 3 lõike 1 punktides a–i loetletud kuriteo toimepanemisega;

8) „tingimused“ – kõik tingimused, mis tahes nimetusega või vormis, mis reguleerivad veebimajutusteenuse pakkuja ja tema teenuse kasutajate lepingulist suhet;

9) „peamine tegevuskoht“ – veebimajutusteenuse pakkuja peakontor või registrijärgne asukoht, kus toimub peamine finantstegevus ja tegevuse juhtimine.

II jagu

Terroristliku veebisisu levitamise vastu võitlemise meetmed

Artikkel 3

Eemaldamiskorraldused

1. Iga liikmesriigi pädeval asutusel on õigus teha eemaldamiskorraldus, millega nõuda veebimajutusteenuse pakkujalt terroristliku sisu eemaldamist või terroristlikule sisule juurdepääsu blokeerimist kõigis liikmesriikides.

2. Kui pädev asutus ei ole veebimajutusteenuse pakkujale varem eemaldamiskorraldust teinud, annab ta vähemalt 12 tundi enne eemaldamiskorralduse tegemist veebimajutusteenuse pakkujale teavet menetluste ja kohaldatavate tähtaegade kohta.

   Esimest lõiku ei kohaldata kohaselt põhjendatud hädaolukordade korral.

3. Veebimajutusteenuse pakkuja eemaldab terroristliku sisu või blokeerib terroristlikule sisule juurdepääsu kõikides liikmesriikides nii kiiresti kui võimalik ja igal juhul hiljemalt ühe tunni jooksul pärast eemaldamiskorralduse kättesaamist.

4. Eemaldamiskorralduse tegemiseks kasutavad pädevad asutused I lisas esitatud vormi. Eemaldamiskorraldus sisaldab järgmisi elemente:

a) eemaldamiskorralduse teinud pädeva asutuse tuvastamisandmeid ja eemaldamiskorralduse autentimist selle pädeva asutuse poolt;

b) piisavalt üksikasjalikku põhjendust, miks asjaomast sisu peetakse terroristlikuks, ja viidet asjakohasele materjali liigile, millele on osutatud artikli 2 punktis 7;

c) täpset ühtset ressursilokaatorit (URL) ja vajaduse korral lisateavet, mille põhjal saaks terroristliku sisu kindlaks teha;

d) viidet käesolevale määrusele kui eemaldamiskorralduse õiguslikule alusele;

e) eemaldamiskorralduse tegemise kuupäeva, ajatemplit ja selle teinud pädeva asutuse elektroonilist allkirja;

f) kergesti arusaadavat teavet veebimajutusteenuse pakkujale ja sisuteenuse pakkujale kättesaadavatest õiguskaitsevahenditest, sealhulgas teavet kuidas pöörduda pädeva asutuse poole ja kohtusse ning teavet kaebuste esitamise tähtaegade kohta;

g) kui see on vajalik ja proportsionaalne, otsust teabe terroristliku sisu eemaldamise või sellele juurdepääsu blokeerimise avalikustamisest loobumise kohta kooskõlas artikli 11 lõikega 3.

5. Pädevad asutused adresseerivad eemaldamiskorralduse veebimajutusteenuse pakkuja peamisesse tegevuskohta või tema seaduslikule esindajale, kelle veebimajutusteenuse pakkuja on määranud vastavalt artiklile 17.

Kõnealune pädev asutus edastab eemaldamiskorralduse artikli 15 lõikes 1 osutatud kontaktpunktile elektroonilisel kujul, mille kohta jääb kirjalik jälg, mis võimaldab autentida saatja ja ka korralduse saatmise ja vastuvõtmise täpse kuupäeva ja kellaaja.

6. Veebimajutusteenuse pakkuja teatab pädevale asutusele põhjendamatu viivituseta ja kasutades selleks II lisas esitatud vormi terroristliku sisu eemaldamisest või terroristlikule sisule juurdepääsu blokeerimisest kõikides liikmesriikides ning märgib eeskätt ära eemaldamise või blokeerimise kellaaja.

7. Kui veebimajutusteenuse pakkuja ei saa eemaldamiskorraldust täita vääramatu jõu tõttu või kuna see on veebimajutusteenuse pakkujast sõltumatutel põhjustel reaalselt võimatu, muu hulgas objektiivselt põhjendatavatel tehnilistel või operatiivsetel põhjustel, teatab ta põhjendamatu viivituseta eemaldamiskorralduse teinud pädevale asutusele need põhjused, kasutades selleks III lisas esitatud vormi.

Lõikes 3 sätestatud tähtaeg hakkab jooksma kohe, kui käesoleva lõike esimeses lõigus osutatud põhjuseid enam ei esine.

8. Kui veebimajutusteenuse pakkuja ei saa eemaldamiskorraldust täita, sest see sisaldab selgeid vigu või ei sisalda korralduse täitmiseks piisavalt teavet, teatab ta sellest põhjendamatu viivituseta eemaldamiskorralduse teinud pädevale asutusele ja küsib vajalikke selgitusi, kasutades selleks III lisas esitatud vormi.

   Lõikes 3 sätestatud tähtaeg hakkab jooksma kohe, kui veebimajutusteenuse pakkuja saab vajalikud selgitused.

9. Eemaldamiskorraldus muutub lõplikuks pärast liikmesriigi õiguse kohase edasikaebamise tähtaja möödumist, kui kaebust ei esitatud, või kui eemaldamiskorraldus on pärast edasikaebamist kinnitatud.

   Kui eemaldamiskorraldus muutub lõplikuks, teatab eemaldamiskorralduse teinud pädev asutus sellest artikli 12 lõike 1 punktis c osutatud pädevale asutusele selles liikmesriigis, kus on veebimajutusteenuse pakkuja peamine tegevuskoht või tema seadusliku esindaja elu- või tegevuskoht.

Artikkel 4

Piiriüleste eemaldamiskorralduste tegemise kord

1. Kui veebimajutusteenuse pakkuja peamine tegevuskoht või seaduslik esindaja ei ole eemaldamiskorralduse teinud pädeva asutuse liikmesriigis, esitab eemaldamiskorralduse teinud pädev asutus samal ajal eemaldamiskorralduse koopia selle liikmesriigi pädevale asutusele, kus on veebimajutusteenuse pakkuja peamine tegevuskoht või tema seadusliku esindaja elu- või tegevuskoht, piiramata seejuures artikli 3 kohaldamist.

2. Kui veebimajutusteenuse pakkuja saab käesolevas artiklis osutatud eemaldamiskorralduse, võtab ta artiklis 3 ettenähtud meetmed ja lisaks meetmed, mis on vajalikud, et asjaomase sisu saaks taastada või võimaldada sellele uuesti juurdepääsu kooskõlas käesoleva artikli lõikega 7.

3. Selle liikmesriigi pädev asutus, kus on veebimajutusteenuse pakkuja peamine tegevuskoht või tema seadusliku esindaja elu- või tegevuskoht võib 72 tunni jooksul alates eemaldamiskorralduse koopia kättesaamisest oma algatusel vastavalt lõikele 1 kontrollida eemaldamiskorraldust, et teha kindlaks, kas sellega rikutakse tõsiselt või ilmselt käesolevat määrust või hartaga tagatud põhiõigusi ja -vabadusi.

   Kui liikmesriigi pädev asutus tuvastab sellise rikkumise, võtab ta sama ajavahemiku jooksul vastu sellekohase põhjendatud otsuse.

4. Veebimajutusteenuse pakkujal ja sisuteenuse pakkujal on õigus esitada 48 tunni jooksul alates eemaldamiskorralduse või artikli 11 lõike 2 kohase teabe saamisest põhjendatud taotlus eemaldamiskorralduse kontrollimiseks vastavalt käesoleva artikli lõike 3 esimesele lõigule selle liikmesriigi pädevale asutusele, kus on veebimajutusteenuse pakkuja peamine tegevuskoht või tema seadusliku esindaja elu- või tegevuskoht.

   Pädev asutus võtab 72 tunni jooksul alates taotluse saamisest pärast eemaldamiskorralduse kontrollimist vastu põhjendatud otsuse, esitades oma järeldused selle kohta, kas rikkumine esineb.

5. Pädev asutus teavitab enne lõike 3 teise lõigu kohase otsuse vastuvõtmist või rikkumise tuvastamise kohta lõike 4 teise lõigu kohase otsuse vastuvõtmist eemaldamiskorralduse teinud pädevat asutust oma kavatsusest otsus vastu võtta ja selle põhjustest.

6. Kui veebimajutusteenuse pakkuja peamise tegevuskoha või tema seadusliku esindaja elu- või tegevuskoha liikmesriigi pädev asutus võtab käesoleva artikli lõike 3 või 4 kohaselt vastu põhjendatud otsuse, edastab ta selle otsuse viivitamata eemaldamiskorralduse teinud asutusele, veebimajutusteenuse pakkujale, sisuteenuse pakkujale, kes taotles käesoleva artikli lõike 4 kohast kontrolli, ja kooskõlas artikliga 14 Europolile. Kui otsuses tuvastatakse käesoleva artikli lõike 3 või 4 kohane rikkumine, kaotab eemaldamiskorraldus õigusliku jõu.

7. Kui asjaomane veebimajutusteenuse pakkuja saab lõike 6 kohase otsuse rikkumise tuvastamise kohta, taastab ta viivitamata sisu või võimaldab sellele uuesti juurdepääsu, ilma et see piiraks tema võimalust nõuda oma tingimuste täitmist kooskõlas liidu ja liikmesriigi õigusega.

Artikkel 5

Erimeetmed

1. Lõikes 4 osutatud terroristliku sisuga kokku puutuv veebimajutusteenuse pakkuja lisab asjaomasel juhul oma tingimustesse sätted, mis käsitlevad tema teenuse kuritarvitamist terroristliku sisu levitamiseks üldsusele, ja kohaldab neid.

Ta teeb seda hoolsalt, proportsionaalselt ja mittediskrimineerivalt ning arvestab kõigis olukordades igakülgselt kasutajate põhiõigustega, võttes eelkõige arvesse väljendus- ja teabevabaduse määravat tähtsust avatud ja demokraatlikus ühiskonnas, et vältida sellise materjali eemaldamist, mis ei ole terroristlik sisu.

2. Kui veebimajutusteenuse pakkuja puutub kokku lõikes 4 osutatud terroristliku sisuga, võtab ta erimeetmeid, et kaitsta oma teenuseid, et neid ei kasutataks terroristliku sisu levitamiseks üldsusele.

Erimeetmete valiku üle otsustab veebimajutusteenuse pakkuja. Sellised meetmed võivad hõlmata ühte või mitut järgmistest:

a) asjakohased tehnilised ja operatiivsed meetmed või suutlikkus, näiteks asjakohane personal või tehnilised vahendid terroristliku sisu kindlakstegemiseks ja kiireks eemaldamiseks või sellele juurdepääsu blokeerimiseks;

b) lihtsalt juurdepääsetavad ja kasutajasõbralikud mehhanismid, mille abil kasutajad saavad veebimajutusteenuse pakkujale teatada väidetavast terroristlikust sisust või selle märgistada;

c) muud mehhanismid, mille eesmärk on suurendada teadlikkust terroristlikust sisust oma teenustes, näiteks kasutajapoolse modereerimise mehhanismid;

d) muud meetmed, mida veebimajutusteenuse pakkuja peab asjakohaseks, et võidelda terroristliku sisu kättesaadavuse vastu oma teenuste kaudu.

3. Erimeetmed peavad vastama kõigile järgmistele nõuetele:

a) nad peavad leevendama tõhusalt veebimajutusteenuse pakkuja terroristliku sisuga kokkupuutumise ulatust;

b) nad peavad olema sihipärased ja proportsionaalsed, võttes eelkõige arvesse veebimajutusteenuse pakkuja terroristliku sisuga kokkupuute ulatuse tõsidust, samuti tehnilist ja operatiivset suutlikkust, rahalist seisu, veebimajutusteenuse pakkuja teenuste kasutajate arvu ja pakutava sisu mahtu;

c) nende kohaldamisel tuleb võtta täiel määral arvesse kasutajate õigusi ja seaduslikku huvi, eelkõige kasutajate põhiõigusi seoses väljendus- ja teabevabadusega, eraelu puutumatuse ja isikuandmete kaitsega;

d) neid tuleb kohaldada hoolsalt ja mittediskrimineerivalt.

Kui erimeetmed hõlmavad tehniliste meetmete kasutamist, tagatakse asjakohased ja tõhusad kaitsemeetmed eelkõige inimeste tehtava jälgimise ja kontrollimise abil, et kindlustada täpsus ja vältida sellise materjali eemaldamist, mis ei ole terroristlik sisu.

4. Veebimajutusteenuse pakkujat käsitatakse terroristliku sisuga kokku puutununa, kui tema peamise tegevuskoha või tema seadusliku esindaja elu- või tegevuskoha liikmesriigi pädev asutus on

   a) teinud otsuse, mis põhineb objektiivsetel teguritel, näiteks sellel, et veebimajutusteenuse pakkuja on viimase 12 kuu jooksul saanud kaks või enam lõplikku eemaldamiskorraldust, ning ta leiab, et veebimajutusteenuse pakkuja on terroristliku sisuga kokku puutunud, ning

   b) veebiteenuse pakkujat punktis a osutatud otsusest teavitanud.

5. Pärast lõikes 4 või asjakohasel juhul lõikes 6 osutatud otsuse saamist esitab veebimajutusteenuse pakkuja pädevale asutusele aruande erimeetmete kohta, mida ta on võtnud ja kavatseb võtta lõigete 2 ja 3 täitmiseks. Ta teeb seda kolme kuu jooksul pärast otsuse kättesaamist ja seejärel igal aastal. See kohustus lõpeb, kui pädev asutus otsustab pärast lõike 7 kohast taotlust, et veebimajutusteenuse pakkuja enam terroristliku sisuga kokku ei puutu.

6. Kui pädev asutus leiab lõikes 5 osutatud aruannete ja asjakohasel juhul muude objektiivsete tegurite alusel, et veebimajutusteenuse pakkuja võetud erimeetmed ei vasta lõigetele 2 ja 3, adresseerib nimetatud pädev asutus veebimajutusteenuse pakkujale otsuse, millega nõutakse temalt vajalike meetmete võtmist, et tagada lõigete 2 ja 3 täitmine.

   Veebimajutusteenuse pakkuja võib otsustada, milliseid erimeetmeid võtta.

7. Veebimajutusteenuse pakkuja võib igal ajal taotleda, et pädev asutus vaataks läbi ja asjakohasel juhul muudaks või tühistaks lõikes 4 või 6 osutatud otsuse.

Pädev asutus võtab kolme kuu jooksul pärast taotluse saamist taotluse kohta vastu otsuse, mis põhineb objektiivsetel teguritel, ning teavitab sellest veebimajutusteenuse pakkujat.

8. Erimeetmete võtmise nõudega ei piirata direktiivi 2000/31/EÜ artikli 15 lõike 1 kohaldamist ning sellega ei kaasne veebimajutusteenuse pakkujatele üldist kohustust seirata teavet, mida nad edastavad või talletavad, ega üldist kohustust otsida aktiivselt ebaseaduslikule tegevusele viitavaid fakte või asjaolusid.

Erimeetmete võtmise nõue ei hõlma veebimajutusteenuse pakkuja kohustust kasutada automaatseid vahendeid.

Artikkel 6

Sisu ja seotud andmete säilitamine

1. Veebimajutusteenuse pakkuja säilitab artiklite 3 ja 5 kohaselt eemaldamiskorralduse või erimeetmete tulemusena eemaldatud või blokeeritud terroristliku sisu ning terroristliku sisu eemaldamise tagajärjel eemaldatud seotud andmed, mis on vajalikud:

a) halduslikus või kohtulikus korras toimuvateks läbivaatamismenetlusteks või kaebuste menetlemiseks vastavalt artiklile 10 seoses otsusega eemaldada terroristlik sisu ja sellega seotud andmed või blokeerida neile juurdepääs, või

b) terroriaktide tõkestamiseks, avastamiseks, uurimiseks või nende eest süüdistuse esitamiseks.

2. Lõikes 1 osutatud terroristlikku sisu ja sellega seotud andmeid säilitatakse kuus kuud peale nende eemaldamist või neile juurdepääsu blokeerimist. Pädeva asutuse või kohtu taotluse korral säilitatakse terroristlikku sisu täiendava kindlaksmääratud ajavahemiku jooksul üksnes juhul kui ja nii kaua kuni see on vajalik lõike 1 punktis a osutatud poolelioleva halduslikus või kohtulikus korras toimuva läbivaatamismenetluse jaoks.

3. Veebimajutusteenuse pakkuja tagab, et vastavalt lõikele 1 säilitatava terroristliku sisu ja sellega seotud andmete suhtes kohaldatakse asjakohaseid tehnilisi ja korralduslikke kaitsemeetmeid.

Tehniliste ja korralduslike kaitsemeetmetega tuleb tagada, et säilitatavale terroristlikule sisule ja sellega seotud andmetele on juurdepääs ja neid saab töödelda ainult lõikes 1 osutatud eesmärgil, ning samuti tuleb tagada asjaomaste isikuandmete turvalisuse kõrge tase. Vajaduse korral vaatavad veebimajutusteenuse pakkujad need kaitsemeetmed üle ja ajakohastavad neid.

III jagu

Kaitsemeetmed ja vastutus

Artikkel 7

Veebimajutusteenuse pakkujate läbipaistvuskohustused

1. Veebimajutusteenuse pakkuja esitab oma tingimustes selgelt terroristliku sisu levitamise vastu võitlemise põhimõtted, sealhulgas asjakohasel juhul sisulise selgituse erimeetmete toimimise, muu hulgas asjakohasel juhul automaatsete vahendite kasutamise kohta.

2. Iga veebimajutusteenuse pakkuja, kes on asjaomasel kalendriaastal võtnud terroristliku sisu levitamise vastaseid meetmeid või kellelt on nõutud meetmete võtmist vastavalt käesolevale määrusele, teeb üldsusele kättesaadavaks läbipaistvusaruande selliste meetmete võtmise kohta antud aastal. Ta avaldab selle aruande enne järgneva aasta 1. märtsi.

3. Läbipaistvusaruanded peavad sisaldama vähemalt järgmist teavet:

   a) teave selle kohta, millised on veebimajutusteenuse pakkuja meetmed terroristliku sisu kindlakstegemiseks ja eemaldamiseks või sellele juurdepääsu blokeerimiseks;

b) teave selle kohta, millised on veebimajutusteenuse pakkuja meetmed sellise veebimaterjali uuesti ilmumise vastu, mis on varem eemaldatud või millele juurdepääs on blokeeritud, sest seda loetakse terroristlikuks sisuks, eelkõige juhul, kui on kasutatud automaatseid vahendeid;

c) nende terroristliku sisu ühikute arv, mis on eemaldatud või millele juurdepääs on blokeeritud kas eemaldamiskorralduse või erimeetmete kohaselt, ning eemaldamiskorralduste arv, mille puhul ei ole sisu eemaldatud või juurdepääsu sellele blokeeritud vastavalt artikli 3 lõike 7 esimesele lõigule ja lõike 8 esimesele lõigule, koos eemaldamata jätmise põhjustega;

d) artiklis 10 osutatud veebimajutusteenuse pakkuja menetletud kaebuste arv ja tulemused;

e) veebimajutusteenuse pakkuja algatatud halduslikus või kohtulikus korras toimuvate läbivaatamismenetluste arv ja tulemused;

f) selliste juhtumite arv, mille puhul veebimajutusteenuse pakkuja oli kohustatud taastama sisu või sellele juurdepääsu halduslikku või kohtuliku läbivaatamismenetluse tulemusena;

g) selliste juhtumite arv, mille puhul veebimajutusteenuse pakkuja taastas sisu või juurdepääsu sellele pärast sisuteenuse pakkuja kaebuse läbivaatamist.

Artikkel 8

Pädevate asutuste läbipaistvusaruanded

1. Pädevad asutused avaldavad igal aastal läbipaistvusaruanded oma käesoleva määruse kohase tegevuse kohta. Kõnealused aruanded sisaldavad asjaomase kalendriaasta kohta vähemalt järgmist teavet:

   a) artikli 3 kohaselt tehtud eemaldamiskorralduste arv, täpsustades artikli 4 lõike 1 reguleerimisalasse jäävate eemaldamiskorralduste arvu, artikli 4 kohaselt kontrollitud eemaldamiskorralduste arvu ning teavet kuidas asjaomased veebimajutusteenuse pakkujad on neid eemaldamiskorraldusi rakendanud, sealhulgas nende juhtumite arv kui terroristlik sisu eemaldati või juurdepääs sellele blokeeriti ning nende juhtumite arv kui terroristlikku sisu ei eemaldatud või juurdepääsu sellele ei blokeeritud;

   b) artikli 5 lõike 4, 6 või 7 kohaselt võetud otsuste arv ja teave nende otsuste rakendamise kohta veebimajutusteenuse pakkujate poolt, sealhulgas kehtestatud erimeetmete kirjeldus;

   c) selliste juhtumite arv, mil eemaldamiskorralduste ning artikli 5 lõigete 4 ja 6 kohaselt vastu võetud otsuste suhtes kohaldati halduslikku või kohtulikku läbivaatamismenetlust, ning teave asjaomaste menetluste tulemuste kohta;

   d) vastavalt artiklis 18 osutatud karistuste määramise otsuste arv, sealhulgas määratud karistusliigi kirjeldus.

2. Lõikes 1 osutatud iga-aastased läbipaistvusaruanded ei sisalda teavet, mis võib mõjutada käimasolevat tegevust terroriaktide tõkestamiseks, avastamiseks, uurimiseks või nende eest süüdistuse esitamiseks, või riikliku julgeoleku huvisid.

Artikkel 9

Õiguskaitsevahendid

1. Veebimajutusteenuse pakkujatel, kes on saanud artikli 3 lõike 1 kohaselt tehtud eemaldamiskorralduse või artikli 4 lõike 4 kohase otsuse või artikli 5 lõike 4, 6 või 7 kohase otsuse, on õigus tõhusale õiguskaitsevahendile. See hõlmab õigust vaidlustada selline eemaldamiskorraldus selle liikmesriigi kohtus, kelle pädev asutus eemaldamiskorralduse tegi, ning õigust vaidlustada artikli 4 lõike 4 või artikli 5 lõike 4, 6 või 7 kohane otsus selle liikmesriigi kohtus, kelle pädev asutus otsuse vastu võttis.

2. Sisuteenuse pakkujatel, kelle sisu on eemaldamiskorralduse alusel eemaldatud või millele juurdepääs on blokeeritud, on õigus tõhusale õiguskaitsevahendile. See hõlmab õigust vaidlustada artikli 3 lõike 1 kohaselt tehtud eemaldamiskorraldus selle liikmesriigi kohtus, kelle pädev asutus eemaldamiskorralduse tegi, ning õigust vaidlustada artikli 4 lõike 4 või artikli 5 lõike 4, 6 või 7 kohane otsus selle liikmesriigi kohtus, kelle pädev asutus otsuse vastu võttis.

3. Liikmesriigid kehtestavad käesolevas artiklis osutatud õiguste kasutamiseks tõhusad meetmed.

Artikkel 10

Kaebuste lahendamise mehhanismid

1. Iga veebimajutusteenuse pakkuja kehtestab mõjusa ja juurdepääsetava mehhanismi, millele toetudes saab sisuteenuse pakkuja, kelle sisu on eemaldatud või kelle sisule juurdepääs on blokeeritud artikli 5 kohaste erimeetmete tõttu, esitada kaebuse sellise eemaldamise või juurdepääsu blokeerimise peale ning nõuda sisu ja juurdepääsu taastamist sellele.

2. Iga veebimajutusteenuse pakkuja vaatab kõik lõikes 1 osutatud mehhanismi kaudu saadud kaebused kiiresti läbi ja kui sisu eemaldamine või juurdepääsu blokeerimine sellele oli alusetu, taastab sisu või juurdepääsu sellele põhjendamatu viivituseta. Ta teavitab kaebuse esitajat kaebuse läbivaatamise tulemustest kahe nädala jooksul alates kaebuse kättesaamisest.

   Kui kaebust ei rahuldata, esitab veebimajutusteenuse pakkuja kaebajale oma otsuse põhjused.

   Sisu või sellele juurdepääsu taastamine ei välista veebimajutusteenuse pakkuja või pädeva asutuse otsuse halduslikku või kohtulikku läbivaatamist.

Artikkel 11

Sisuteenuse pakkujatele esitatav teave

1. Kui veebimajutusteenuse pakkuja on terroristliku sisu eemaldanud või juurdepääsu sellele blokeerinud, teeb ta sisuteenuse pakkujale kättesaadavaks teabe sellise eemaldamise või juurdepääsu blokeerimise kohta.

2. Sisuteenuse pakkuja taotluse korral teavitab veebimajutusteenuse pakkuja sisuteenuse pakkujat eemaldamise või juurdepääsu blokeerimise põhjustest ja tema õigustest eemaldamiskorraldus vaidlustada või esitab sisuteenuse pakkujale tehtud eemaldamiskorralduse koopia.

3. Lõigete 1 ja 2 kohast kohustust ei kohaldata, kui eemaldamiskorralduse teinud pädev asutus otsustab, et avalikustamisest loobumine on vajalik ja proportsionaalne avaliku julgeolekuga seotud põhjustel, näiteks terroriaktide tõkestamiseks, uurimiseks, avastamiseks ja nende eest süüdistuse esitamiseks, nii kauaks kui vaja, aga mitte kauem kui kuue nädala jooksul alates kõnealuse otsuse tegemisest. Sellisel juhul ei avalikusta veebimajutusteenuse pakkuja terroristliku sisu eemaldamise või sellele juurdepääsu tõkestamise kohta mingit teavet.

   Nimetatud pädev asutus võib sellise avalikustamata jätmise ajavahemikku pikendada veel kuue nädala võrra, kui see on jätkuvalt põhjendatud.

IV jagu

Pädevad asutused ja koostöö

Artikkel 12

Pädevate asutuste määramine

1. Iga liikmesriik määrab asutuse või asutused, kelle pädevusse kuulub:

   a) eemaldamiskorralduste tegemine vastavalt artiklile 3;

   b) eemaldamiskorralduste kontrollimine vastavalt artiklile 4;

   c) erimeetmete rakendamise jälgimine vastavat artiklile 5;

   d) karistuste kehtestamine vastavalt artiklile 18.

2. Iga liikmesriik tagab, et lõike 1 punktis a osutatud pädeva asutuste juurde on määratud või asutatud kontaktpunkt, kes tegeleb selle pädeva asutuse tehtud eemaldamiskorralduse kohta esitatud selgitamisnõuete ja tagasisidega.

   Liikmesriik tagab, et teave kontaktpunkti kohta tehakse avalikult kättesaadavaks.

3. Hiljemalt … [12 kuud pärast käesoleva määruse jõustumist] teatavad liikmesriigid komisjonile lõikes 1 osutatud pädeva asutuse või pädevate asutuste nimed ja kõigist nende muudatustest. Komisjon avaldab saadud teate ja selle muudatused *Euroopa Liidu Teatajas*.

4. Komisjon loob hiljemalt … [12 kuud pärast käesoleva määruse jõustumist] veebiregistri, milles on loetletud lõikes 1 osutatud pädevad asutused ja lõike 2 kohaselt iga pädeva asutuse juurde määratud või asutatud kontaktpunkt. Komisjon avaldab korrapäraselt kõik nende muudatused.

Artikkel 13

Pädevad asutused

1. Liikmesriigid tagavad, et nende pädevatel asutustel on vajalikud volitused ja piisavad ressursid, et saavutada eesmärgid ja täita kohustused, mis tulenevad käesolevast määrusest.

2. Liikmesriigid tagavad, et pädevad asutused täidavad oma käesolevast määrusest tulenevaid ülesandeid objektiivsel ja mittediskrimineerival viisil, austades täiel määral põhiõigusi. Pädevad asutused ei taotle ega võta vastu juhiseid üheltki teiselt organilt seoses artikli 12 lõike 1 kohaste ülesannete täitmisega.

Käesoleva lõike esimene lõik ei välista liikmesriigi riigiõiguse kohast järelevalvet.

Artikkel 14

Veebimajutusteenuse pakkujate, pädevate asutuste ja Europoli koostöö

1. Seoses eemaldamiskorraldustega vahetavad pädevad asutused teavet, koordineerivad ja teevad koostööd omavahel ning asjakohasel juhul Europoliga, et vältida topelttööd, parandada koordineerimist ja vältida sekkumist teistes liikmesriikides toimuvatesse uurimistesse.

2. Artikli 5 kohaselt võetud erimeetmete ja artikli 18 kohaselt kehtestatud karistuste puhul vahetavad liikmesriikide pädevad asutused teavet, koordineerivad ja teevad koostööd artikli 12 lõike 1 punktides c ja d osutatud pädevate asutusetega. Liikmesriigid tagavad, et artikli 12 lõike 1 punktides c ja d osutatud pädevate asutuste käsutuses on kogu asjakohane teave.

3. Lõike 1 kohaldamisel näevad liikmesriigid ette asjakohased ja turvalised sidekanalid ja -mehhanismid, et tagada asjaomase teabe õigeaegne jagamine.

4. Käesoleva määruse tõhusaks rakendamiseks ja topelttöö vältimiseks võivad liikmesriigid ja veebimajutusteenuse pakkujad otsustada kasutada spetsiaalseid vahendeid, sealhulgas Europoli loodud vahendeid, et aidata kaasa eeskätt järgmisele tegevusele:

   a) artikli 3 kohaste eemaldamiskorralduste töötlemine ja nendega seotud tagasiside ning

   b) koostöö, et määrata kindlaks ja rakendada artikli 5 kohaseid erimeetmeid.

5. 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 tuvastada, teavitavad veebimajutusteenuse pakkujad artikli 12 lõike 2 kohast kontaktpunkti liikmesriigis, kus on nende peamine tegevuskoht või nende seadusliku esindaja elu- või tegevuskoht, ning edastavad teabe sellise terroristliku sisu kohta Europolile asjakohaste järelmeetmete võtmiseks.

6. Pädevatel asutustel soovitatakse saata Europolile eemaldamiskorralduste koopiad, mis võimaldavad tal esitada aastaaruande, mis sisaldab analüüsi terroristliku sisu liikide kohta, mille suhtes kohaldatakse käesoleva määruse kohaselt eemaldamiskorraldust või juurdepääsu blokeerimist.

Artikkel 15

Veebimajutusteenuse pakkujate kontaktpunktid

1. Iga veebimajutusteenuse pakkuja määrab või asutab kontaktpunkti, mille kaudu võtta elektrooniliselt vastu eemaldamiskorraldusi ning tagada nende kiire töötlemine vastavalt artiklitele 3 ja 4. Veebimajutusteenuse pakkuja tagab, et teave kontaktpunktide kohta on avalikult kättesaadav.

2. Käesoleva artikli lõikes 1 osutatud teabes tuleb ära märkida määruses nr 1/58[1] nimetatud liidu institutsioonide ametlikud keeled, milles võib kontaktpunkti poole pöörduda ja mida kasutatakse edasiseks suhtlemiseks artikli 3 kohaste eemaldamiskorralduste puhul. Nende keelte hulka peab kuuluma vähemalt üks selle liikmesriigi ametlik keel, kus on veebimajutusteenuse pakkuja peamine tegevuskoht või kus on tema seadusliku esindaja elu- või tegevuskoht.

[1] Nõukogu määrus nr 1, millega määratakse kindlaks Euroopa Majandusühenduses kasutatavad keeled (EÜT 17, 6.10.1958, lk 385).

V jagu

Rakendamine ja täitmise tagamine

Artikkel 16

Jurisdiktsioon

1. Artiklite 5, 18 ja 21 kohaldamisel on jurisdiktsioon liikmesriigil, kus on veebimajutusteenuse pakkuja peamine tegevuskoht. Kui veebimajutusteenuse pakkuja peamine tegevuskoht ei ole liidus, loetakse ta selle liikmesriigi jurisdiktsiooni alla kuuluvaks, kus on tema seadusliku esindaja elu- või tegevuskoht.

2. Kui veebimajutusteenuse pakkuja, kelle peamine tegevuskoht ei ole liidus, ei suuda seaduslikku esindajat määrata, saavad jurisdiktsiooni teostada kõik liikmesriigid.

3. Kui liikmesriigi pädev asutus otsustab vastavalt lõikele 2 oma jurisdiktsiooni teostada, teavitab ta kõigi teiste liikmesriikide pädevaid asutusi.

Artikkel 17

Seaduslik esindaja

1. Veebimajutusteenuse pakkuja, kelle peamine tegevuskoht ei ole liidus, määrab kirjalikult oma seaduslikuks esindajaks liidus füüsilise või juriidilise isiku, et see tegeleks pädevate asutuste tehtud eemaldamiskorralduste ja otsuste kättesaamise, järgimise ja täitmise tagamisega.

2. Veebimajutusteenuse pakkuja annab oma seaduslikule esindajale vajalikud õigused ja vahendid, et ta saaks täita kõnealuseid eemaldamiskorraldusi ja otsuseid ning teha pädevate asutustega koostööd.

Seaduslik esindaja elu-või tegevuskoht on ühes liikmesriikidest, kus veebimajutusteenuse pakkuja teenuseid pakub.

3. Käesoleva määruse rikkumise eest võib seadusliku esindaja vastutusele võtta, ilma et see piiraks veebimajutusteenuse pakkuja vastutust ega kohtuvaidlusi.

4. Veebimajutusteenuse pakkuja teatab määramisest oma seadusliku esindaja elu- või tegevuskoha liikmesriigi artikli 12 lõike 1 punktis d osutatud pädevale asutusele.

Veebimajutusteenuse pakkuja teeb teabe seadusliku esindaja kohta avalikult kättesaadavaks.

VI jagu

Lõppsätted

Artikkel 18

Karistused

1. Liikmesriigid kehtestavad veebimajutusteenuse pakkuja poolt käesoleva määruse rikkumise eest kohaldatavad karistusnormid ja võtavad kõik vajalikud meetmed nende rakendamise tagamiseks. Karistusi kohaldatakse üksnes artikli 3 lõigete 3 ja 6, artikli 4 lõigete 2 ja 7, artikli 5 lõigete 1, 2, 3, 5 ja 6, artiklite 6, 7, 10 ja 11, artikli 14 lõike 5, artikli 15 lõike 1 ja artikli 17 rikkumise korral.

   Esimeses lõigus osutatud karistused peavad olema tõhusad, proportsionaalsed ja hoiatavad. Liikmesriigid teatavad komisjoni hiljemalt … [12 kuu jooksul pärast käesoleva määruse jõustumist] kõnealustest normidest ja meetmetest ning teavitavad teda viivitamata nende hilisematest muudatustest.

2. Liikmesriigid tagavad, et karistuse määramise üle otsustamisel ning karistuste liigi ja määra kindlaksmääramisel võtavad pädevad asutused arvesse kõiki asjaomaseid asjaolusid, muu hulgas järgmist:

   a) rikkumise laadi, raskust ja kestust;

   b) kas rikkumine pandi toime tahtlikult või hooletusest;

c) veebimajutusteenuse pakkuja varasemaid rikkumisi;

d) veebimajutusteenuse pakkuja rahalist seisu;

e) veebimajutusteenuse pakkuja valmidust teha pädevate asutustega koostööd ;

f) veebimajutusteenuse pakkuja laadi ja suurust, eelkõige seda, kas ta on mikro-, väikese või keskmise suurusega ettevõtja;

g) veebimajutusteenuse pakkuja süü määra, võttes arvesse tehnilisi ja korralduslikke meetmeid, mida veebimajutusteenuse pakkuja on võtnud käesoleva määruse täitmiseks.

3. Liikmesriigid tagavad, et artikli 3 lõikest 3 tulenevate kohustuste süstemaatilise või korduva eiramise korral rakendatakse rahalist karistust, mille summa on kuni 4 % veebimajutusteenuse pakkuja eelmise majandusaasta kogukäibest.

Artikkel 19

Tehnilised nõuded ja lisade muutmine

1. Komisjonil on õigus võtta kooskõlas artikliga 20 vastu delegeeritud õigusakte, et täiendada käesolevat määrust vajalike tehniliste nõuetega elektrooniliste vahendite kohta, mida pädevad asutused peavad kasutama eemaldamiskorralduste edastamiseks.

2. Komisjonil on õigus võtta kooskõlas artikliga 20 vastu delegeeritud õigusakte lisade muutmiseks, et tegeleda võimaliku vajadusega parandada eemaldamiskorralduse vormide sisu ning anda teada eemaldamiskorralduse täitmise võimatusest.

Artikkel 20

Delegeeritud volituste rakendamine

1. Komisjonile antakse õigus võtta vastu delegeeritud õigusakte käesolevas artiklis sätestatud tingimustel.

2. Artiklis 19 osutatud õigus võtta vastu delegeeritud õigusakte antakse komisjonile määramata ajaks alates … [üks aasta pärast käesoleva määruse jõustumise kuupäeva].

3. Euroopa Parlament ja nõukogu võivad artiklis 19 osutatud volituste delegeerimise igal ajal tagasi võtta. Tagasivõtmise otsusega lõpetatakse otsuses nimetatud volituste delegeerimine. Otsus jõustub järgmisel päeval pärast selle avaldamist *Euroopa Liidu Teatajas* või otsuses nimetatud hilisemal kuupäeval. See ei mõjuta juba jõustunud delegeeritud õigusaktide kehtivust.

4. Enne delegeeritud õigusakti vastuvõtmist konsulteerib komisjon kooskõlas 13. aprilli 2016. aasta institutsioonidevahelises parema õigusloome kokkuleppes sätestatud põhimõtetega iga liikmesriigi määratud ekspertidega.

5. Niipea kui komisjon on delegeeritud õigusakti vastu võtnud, teeb ta selle samal ajal teatavaks Euroopa Parlamendile ja nõukogule.

6. Artikli 19 alusel vastu võetud delegeeritud õigusakt jõustub üksnes juhul, kui Euroopa Parlament ega nõukogu ei ole kahe kuu jooksul pärast õigusakti teatavakstegemist Euroopa Parlamendile ja nõukogule esitanud selle suhtes vastuväidet või kui Euroopa Parlament ja nõukogu on enne selle tähtaja möödumist komisjonile teatanud, et nad ei esita vastuväidet. Euroopa Parlamendi või nõukogu algatusel pikendatakse seda tähtaega kahe kuu võrra.

Artikkel 21

Seire

1. Liikmesriigid koguvad oma pädevatelt asutustelt ja oma jurisdiktsiooni alla kuuluvatelt veebimajutusteenuse pakkujatelt teavet eelmisel kalendriaastal käesoleva määruse kohaselt võetud meetmete kohta ning saadavad selle teabe komisjonile iga aasta 31. märtsiks. Kõnealune teave hõlmab järgmist:

   a) tehtud eemaldamiskorralduste arv ja terroristliku sisu ühikute arv, mis on eemaldatud või millele juurdepääs on blokeeritud, ning eemaldamise või juurdepääsu blokeerimise kiirus;

   b) erimeetmed, mis on võetud vastavalt artiklile 5, kaasa arvatud terroristliku sisu ühikute arv, mis on eemaldatud või millele juurdepääs on blokeeritud, ning eemaldamise või juurdepääsu blokeerimise kiirus;

c) mitu juurdepääsutaotlust on pädevad asutused teinud seoses veebimajutusteenuse pakkujate poolt vastavalt artiklile 7 säilitatud sisuga;

d) mitu kaebuste lahendamise menetlust on algatatud ja kui palju meetmeid on veebimajutusteenuse pakkujad võtnud vastavalt artiklile 10;

e) mitu halduslikku või kohtulikku läbivaatamismenetlust on algatatud ja millised otsused on pädev asutus liikmesriigi õiguse alusel teinud.

2. Komisjon koostab hiljemalt … [kaks aastat pärast käesoleva määruse jõustumise kuupäeva] käesoleva määruse väljundite, tulemuste ja mõju seiramiseks üksikasjaliku kava. Seirekavas sätestatakse andmete ja muu vajaliku tõendusmaterjali kogumisel kasutatavad näitajad ja vahendid ning kogumise sagedus. Kavas täpsustatakse, millised on komisjoni ja liikmesriikide ülesanded andmete ja muu tõendusmaterjali kogumisel ja analüüsimisel, et seirata edusamme ja hinnata käesolevat määrust vastavalt artiklile 23.

Artikkel 22

Rakendamisaruanne

Hiljemalt … [kaks aastat pärast käesoleva määruse jõustumist] esitab komisjon Euroopa Parlamendile ja nõukogule aruande käesoleva määruse kohaldamise kohta. See aruanne sisaldab teavet artikli 21 kohase seire kohta ja artikli 8 kohastest läbipaistvuskohustustest tulenevat teavet. Liikmesriigid esitavad komisjonile teabe, mida on vaja aruande kava koostamiseks.

Artikkel 23

Hindamine

Hiljemalt … [kolm aastat pärast käesoleva määruse jõustumise kuupäeva] hindab komisjon käesolevat määrust ning esitab Euroopa Parlamendile ja nõukogule aruande selle kohaldamise kohta, sealhulgas

a) kaitsemehhanismide, eelkõige artikli 4 lõikes 4, artikli 6 lõikes 3 ja artiklites 7–11 osutatud kaitsemehhanismide toimimise ja tõhususe kohta,

b) käesoleva määruse kohaldamise mõju kohta põhiõigustele, eelkõige väljendus- ja teabevabadusele, eraelu puutumatusele ja isikuandmete kaitsele, ning

c) käesoleva määruse panuse kohta avaliku julgeoleku kaitsesse.

Asjakohasel juhul esitatakse koos aruandega seadusandlikud ettepanekud.

Liikmesriigid esitavad komisjonile aruande koostamiseks vajaliku teabe.

Komisjon hindab ka käesoleva määruse alusel teabevahetuse ja koostöö hõlbustamiseks terroristliku veebisisu Euroopa platvormi loomise vajalikkust ja teostatavust.

Artikkel 24

Jõustumine ja kohaldamine

Käesolev määrus jõustub kahekümnendal päeval pärast selle avaldamist *Euroopa Liidu Teatajas*.

Seda kohaldatakse alates … [12 kuud pärast käesoleva määruse jõustumist].

Käesolev määrus on tervikuna siduv ja vahetult kohaldatav kõikides liikmesriikides.

…,

Euroopa Parlamendi nimel	*Nõukogu nimel*
president	*eesistuja*

I LISA

EEMALDAMISKORRALDUS (Euroopa Parlamendi ja nõukogu määruse (EL) 2021/…

artikkel 3[+])

Vastavalt määruse (EL) 2021/… [++] artiklile 3 (edaspidi „määrus“) eemaldab eemaldamiskorralduse adressaat terroristliku sisu või blokeerib terroristlikule sisule juurepääsu kõikides liikmesriikides nii kiiresti kui võimalik ja igal juhul ühe tunni jooksul pärast seda, kui ta on saanud kätte eemaldamiskorralduse. Vastavalt määruse artiklile 6 peavad adressaadid säilitama sisu ja sellega seotud andmeid, mis on eemaldatud või millele juurdepääs on blokeeritud, kuus kuud või kauem, kui seda on taotlenud pädev asutus või kohus. Vastavalt määruse artikli 15 lõikele 2 tuleb eemaldamiskorraldus teha ühes neist keeltes, mille adressaat on määranud.

[+] ELT: palun sisestada teksti dokumendis ST 14308/20 (2018/0331(COD)) sisalduva määruse number ning esitada joonealuses märkuses kõnealuse määruse kuupäev, number, pealkiri ja ELT avaldamisviide.

[++] ELT: palun sisestada teksti dokumendis ST 14308 /20 (2018/0331(COD)) sisalduva määruse number.

A JAGU

Eemaldamiskorralduse teinud pädeva asutuse liikmesriik:

……..……..

NB! eemaldamiskorralduse teinud pädeva asutuse või ametiisiku andmed, mis esitatakse E ja F jaos.

Adressaat ja asjakohasel juhul seaduslik esindaja:

……..……..

Kontaktpunkt:

……..……..

Liikmesriik, kus on veebimajutusteenuse pakkuja peamine tegevuskoht või kus on tema seadusliku esindaja elu- või tegevuskoht:

……..……..

Eemaldamiskorralduse tegemise kellaaeg ja kuupäev:

……..……..

Eemaldamiskorralduse viitenumber:

……..……..

B JAGU Terroristlik sisu, mis tuleb eemaldada või millele juurdepääs tuleb blokeerida kõikides liikmesriikides nii kiiresti kui võimalik ja igal juhul ühe tunni jooksul pärast eemaldamiskorralduse kättesaamist:

URL ja igasugune lisateave, mis võimaldab esildise objektiks oleva terroristliku sisu kindlaks teha ja määrata selle täpse asukoha:

……..……

Põhjused, miks materjali peetakse terroristlikuks sisuks kooskõlas käesoleva määruse artikli 2 punktiga 7.

Materjal (palun teha märge vastavasse lahtrisse / vastavatesse lahtritesse):

□ õhutab teisi terroriakte toime panema, näiteks ülistades terroriakte ning õigustades selliste kuritegude toimepanekut (käesoleva määruse artikli 2 punkti 7 alapunkt a)

□ ärgitab teisi terroriakte toime panema või aitab nende toimepanemisele kaasa (käesoleva määruse artikli 2 punkti 7 alapunkt b)

□ ärgitab teisi osalema terrorirühmituse tegevuses (käesoleva määruse artikli 2 punkti 7 alapunkt c)

□ annab juhiseid lõhkeainete, tuli- või muude relvade või mürgiste või ohtlike ainete valmistamise või kasutamise kohta või muude konkreetsete meetodite või tehniliste võtete kohta terroriakti toimepanemise või sellele kaasa aitamise eesmärgil (käesoleva määruse artikli 2 punkti 7 alapunkt d)

□ kujutab endast terroriakti toimepanemise ohtu (käesoleva määruse artikli 2 punkti 7 alapunkt e).

Lisateave põhjuste kohta, miks materjali peetakse terroristlikuks sisuks:
……..
……..
…….

C JAGU Teave sisuteenuse pakkujale

Palun panna tähele, et (palun teha märge vastavasse lahtrisse, kui see on asjakohane):

□ avaliku julgeolekuga seotud põhjustel **ei tohi adressaat teavitada sisuteenuse pakkujat** terroristliku sisu eemaldamisest või sellele juurdepääsu blokeerimisest.

kui see lahter ei ole asjakohane, palun vaadata G jaost üksikasju võimaluste kohta vaidlustada eemaldamiskorraldus liikmesriigi õiguse kohaselt selle teinud pädeva asutuse liikmesriigis (eemaldamiskorralduse koopia tuleb taotluse korral saata sisuteenuse pakkujale).

D JAGU Teave selle liikmesriigi pädeva asutuse kohta, kus on veebimajutusteenuse pakkuja peamine tegevuskoht või tema seadusliku esindaja elu- või tegevuskoht

Palun teha märge vastavasse lahtrisse / vastavatesse lahtritesse:

□ Liikmesriik, kus on veebimajutusteenuse pakkuja peamine tegevuskoht või kus on tema seadusliku esindaja elu- või tegevuskoht, ei ole sama kui eemaldamiskorralduse teinud pädeva asutuse liikmesriik

□ Eemaldamiskorralduse koopia on saadetud selle liikmesriigi pädevale asutusele, kus on veebimajutusteenuse pakkuja peamine tegevuskoht või tema seadusliku esindaja elu- või tegevuskoht

E JAGU Eemaldamiskorralduse teinud pädeva asutuse andmed

Asutuse liik (palun teha märge vastavasse lahtrisse):

□ kohtunik, kohus või eeluurimiskohtunik

□ õiguskaitseasutus

□ muu pädev asutus → palun täita ka F jagu.

Andmed eemaldamiskorralduse teinud pädeva asutuse või tema esindaja kohta, kes kinnitab eemaldamiskorralduse täpsust ja õigsust

Eemaldamiskorralduse teinud pädeva asutuse nimi:
……..……..

Tema esindaja nimi ja ametikoht (nimetus/ametiaste):
……..……..

Toimiku nr: ….……..……..……..

Aadress: …….……..……..

Telefon (riigi kood) (piirkonna/linna sihtnumber): .....

Faks (riigi kood) (piirkonna/linna sihtnumber): .....

E-posti aadress: ……..……..……...

Kuupäev:…….……

Ametlik tempel (kui see on olemas) ja allkiri[1]: ……...……

[1] Allkirja ei ole vaja, kui eemaldamiskorraldus on saadetud autenditud edastuskanalite kaudu, mis tagab eemaldamiskorralduse autentsuse.

F JAGU Kontaktandmed toimiku edasiseks menetlemiseks

Eemaldamiskorralduse teinud pädeva asutuse kontaktandmed tagasiside andmiseks sisu eemaldamise või sellele juurdepääsu blokeerimise aja kohta või täiendavate selgituste esitamiseks:

……..…….

Selle liikmesriigi pädeva asutuse kontaktandmed, kus on veebimajutusteenuse pakkuja peamine tegevuskoht või kus on tema seadusliku esindaja elu- või tegevuskoht:

……..…….

G JAGU Teave õiguskaitsevõimaluste kohta

Teave pädeva asutuse või kohtu ning eemaldamiskorralduse vaidlustamise tähtaegade ja menetluste kohta:

Pädev asutus või kohus, kus saab eemaldamiskorralduse vaidlustada:

……..…….

Eemaldamiskorralduse vaidlustamise tähtaeg:

[päeva/kuud alates]

……

Viide liikmesriigi õigusaktide sätetele:

……..…….

II LISA

TAGASISIDE PÄRAST TERRORISTLIKU SISU EEMALDAMIST
VÕI SELLELE JUURDEPÄÄSU BLOKEERIMIST
(Euroopa Parlamendi ja nõukogu
määruse (EL) 2021/… artikli 3 lõige 6[+])

A JAGU

Eemaldamiskorralduse adressaat:

……..……..

Eemaldamiskorralduse teinud pädev asutus:

……..……..

Eemaldamiskorralduse teinud pädeva asutuse registrinumber:

……..……..

Adressaadi registrinumber:

……..……..

Eemaldamiskorralduse kättesaamise kellaaeg ja kuupäev:

……..……..

[+] ELT: palun sisestada teksti dokumendis ST 14308 /20 (2018/0331(COD)) sisalduva määruse number ning esitada joonealuses märkuses kõnealuse määruse kuupäev, number, pealkiri ja ELT avaldamisviide.

B JAGU

Eemaldamiskorralduse kohaselt võetud meetmed

(palun teha märge vastavasse lahtrisse):

□ terroristlik sisu on eemaldatud

□ juurdepääs terroristlikule sisule on blokeeritud kõikides liikmesriikides

Võetud meetme kellaaeg ja kuupäev: ……..

C JAGU Adressaadi andmed

Veebimajutusteenuse pakkuja nimi:

……

VÕI

Veebimajutusteenuse pakkuja seadusliku esindaja nimi:

……..……..

Veebimajutusteenuse pakkuja peamise tegevuskoha liikmesriik:

……

VÕI

Veebimajutusteenuse pakkuja seadusliku esindaja elu- või tegevuskoha liikmesriik:

……..……..

Volitatud isiku nimi:

……..……..

Kontaktpunkti e-posti aadress:

…….

Kuupäev:

……..……..

III LISA

TEAVE EEMALDAMISKORRALDUSE
TÄITMISE VÕIMATUSE KOHTA
(Euroopa Parlamendi ja nõukogu
määruse (EL) 2021/…[+] artikli 3 lõiked 7 ja 8)

A JAGU

Eemaldamiskorralduse adressaat:

……..……..

Eemaldamiskorralduse teinud pädev asutus:

……..……..

Eemaldamiskorralduse teinud pädeva asutuse registrinumber:

……..……..

Adressaadi registrinumber:

……..……..

Eemaldamiskorralduse kättesaamise kellaaeg ja kuupäev:

……..……..

[+] ELT: palun sisestada teksti dokumendis ST 14308 /20 (2018/0331(COD)) sisalduva määruse number ning esitada joonealuses märkuses kõnealuse määruse kuupäev, number, pealkiri ja ELT avaldamisviide.

B JAGU Täitmata jätmine

1) Eemaldamiskorraldust ei ole võimalik täita nõutud tähtaja jooksul järgmistel põhjustel (palun teha märge vastavasse lahtrisse / vastavatesse lahtritesse):

□ vääramatu jõud või objektiivne võimatus, mis ei sõltu veebimajutusteenuse pakkujast, muu hulgas objektiivselt põhjendatavatel tehnilistel või operatiivsetel põhjustel

□ eemaldamiskorraldus sisaldab ilmseid vigu

□ eemaldamiskorralduses esitatud teave ei ole piisav

2) Palun esitada lisateave täitmata jätmise põhjuste kohta:

…….

3) Kui eemaldamiskorralduses on ilmsed vead ja/või selles esitatud teave ei ole piisav, palun täpsustada, millised need vead on ja millist lisateavet või täiendavaid selgitusi on tarvis:

…….

C JAGU Veebimajutusteenuse pakkuja või tema seadusliku esindaja andmed

Veebimajutusteenuse pakkuja nimi:

……..……..

VÕI

Veebimajutusteenuse pakkuja seadusliku esindaja nimi:

……..……..

Volitatud isiku nimi:

……..……..

Kontaktandmed (e-posti aadress):

……..……..

Allkiri:

……..……..

Kellaaeg ja kuupäev:

……..……..