Euroopa Liidu
Nõukogu

Brüssel, 7. detsember 2018
(OR. en)

15336/18

Institutsioonidevaheline dokument: 2018/0331(COD)

CT 198
ENFOPOL 605
JAI 1264
COTER 175
CYBER 313
TELECOM 461
FREMP 222
AUDIO 121
DROIPEN 199
CODEC 2270

MENETLUSE TULEMUS

Saatja:	Nõukogu peasekretariaat
Kuupäev:	6. detsember 2018
Saaja:	Delegatsioonid
Eelmise dok nr:	14978/18 + COR 1
Komisjoni dok nr:	12129/18 + ADD 1-3
Teema:	Ettepanek: Euroopa Parlamendi ja nõukogu määrus terroristliku veebisisu levitamise tõkestamise kohta – üldine lähenemisviis

Nõukogu leppis 6. detsembril 2018 kokku lisas esitatud üldises lähenemisviisis.

Komisjoni ettepanekusse tehtud muudatused on märgitud ***paksus kaldkirjas*** ja väljajäetud kohad on tähistatud nurksulgudega […].

[…]

[…] ***Eelnõu:***

EUROOPA PARLAMENDI JA NÕUKOGU MÄÄRUS

terroristliku veebisisu levitamise tõkestamise kohta

[…]

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

ning arvestades järgmist:

(1) Käesoleva määruse eesmärk on tagada veebimajutusteenuste terrorismiotstarbelise kuritarvitamise tõkestamise kaudu 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 võrgukeskkonna vastu ning sõna- ja teabevabaduse kaitsemeetmete tugevdamine.

[1] ELT C ..., ..., lk …

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

(3) Terroristlikul veebisisul on tõsised negatiivsed tagajärjed nii kasutajate, kodanike ja laiema ühiskonna kui ka sellist sisu majutavate internetipõhiste teenuste osutajate jaoks, sest see õõnestab nende kasutajate usaldust ja kahjustab nende ärimudeleid. Arvestades internetipõhiste teenuste osutajate keskset rolli ja nende osutatavate teenustega seotud tehnoloogilisi vahendeid ja võimalusi, on neil teatav ühiskondlik kohustus kaitsta oma teenuseid terroristidepoolse kuritarvitamise eest ning aidata võidelda terroristliku sisu vastu, mida levitatakse nende teenuseid kasutades.

(4) Liidu tasandil alustati võitlust terroristliku veebisisu vastu 2015. aastal liikmesriikide ja veebimajutusteenuse pakkujate vabatahtliku koostööraamistiku alusel, kuid nüüd tuleks seda täiendada selge õigusraamistikuga, et veelgi vähendada juurdepääsu terroristlikule veebisisule ja leida sellele kiirelt arenevale probleemile otstarbekad lahendused. Nimetatud õigusraamistik tugineb vabatahtlikule tööle, mida komisjon on toetanud oma soovituses (EL) 2018/334,[2] ning see on vastus Euroopa Parlamendi üleskutsetele kasutada võitluses ebaseadusliku ja kahjuliku infosisu vastu jõulisemaid meetmeid ja parandada terroriaktidele õhutava sisu automaatset avastamist ja eemaldamist.

[2] 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).

(5) Käesoleva määruse kohaldamine ei tohiks mõjutada direktiivi 2000/31/EÜ[3] artikli 14 kohaldamist. Ennekõike ei tohiks ükski meede, sealhulgas ennetusmeede, mille veebimajutusteenuse pakkuja võtab kooskõlas käesoleva määrusega, takistada kõnealust teenusepakkujat kasutamast nimetatud artikli kohast vastutusest vabastamise erandit. Käesolev määrus ei mõjuta liikmesriikide ametiasutuste ja kohtute õigust teha veebimajutusteenuse pakkuja vastutus kindlaks konkreetsetel juhtudel, kui direktiivi 2000/31/EÜ artiklis 14 sätestatud vastutusest vabastamise erandi tingimused ei ole täidetud. ***Käesolevat määrust ei kohaldata riikliku julgeolekuga seotud tegevuste suhtes, kuna need kuuluvad iga liikmesriigi ainuvastutusse.***

(6) Käesoleva määrusega nähakse ette õigusnormid, mille abil tõkestada veebimajutusteenuste kuritarvitamist terroristliku veebisisu levitamiseks, et tagada siseturu tõrgeteta toimimine, austades seejuures täielikult liidu õiguskorra kohaselt kaitstud põhiõigusi, eelkõige Euroopa Liidu põhiõiguste hartaga tagatud õigusi.

[3] 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).

(7) Käesoleva määrusega aidatakse kaitsta avalikku julgeolekut ning kehtestatakse asjakohased ja töökindlad kaitsemeetmed, et tagada asjaomaste põhiõiguste kaitse. Need hõlmavad õigust eraelu puutumatusele ja isikuandmete kaitsele, õigust tõhusale kohtulikule kaitsele, õigust sõnavabadusele, kaasa arvatud vabadust saada ja anda teavet, ettevõtlusvabadust ja mittediskrimineerimise põhimõtet. Pädevad asutused ja veebimajutusteenuse pakkujad peaksid võtma üksnes selliseid meetmeid, mis on demokraatlikus ühiskonnas vajalikud, asjakohased ja proportsionaalsed, võttes arvesse seda, kui oluliseks peetakse sõna- ja teabevabadust, ***samuti ajakirjandusvabadust ja meedia mitmekesisust***, mis on pluralistliku demokraatliku ühiskonna [...] [...] põhialuseks ning üks liidu alusväärtusi. Meetmed, millega sekkutakse sõna- ja teabevabadusse, peaksid olema rangelt sihipärased selles mõttes, et nende eesmärk peab olema tõkestada terroristliku sisu levitamist, kuid selle käigus ei tohi kahjustada õigust seaduslikult teavet saada ja levitada, võttes arvesse veebimajutusteenuse pakkujate keskset rolli avalikule arutelule ning faktide, arvamuste ja ideede õiguspärasele levitamisele kaasaaitamisel.

(8) Euroopa Liidu lepingu artiklis 19 ja Euroopa Liidu põhiõiguste 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 kahjustavad selle isiku õigusi. See õigus hõlmab veebimajutusteenuse ja sisuteenuse pakkujate jaoks võimalust vaidlustada eemaldamiskorraldus selle liikmesriigi kohtus, kelle ametiasutus eemaldamiskorralduse tegi ***ning veebimajutusteenuse pakkujate jaoks võimalust vaidlustada ennetavate meetmete või karistuste määramise otsus selle liikmesriigi kohtus, kus teenusepakkuja asub või kus tal on esindaja.***

(9) Et oleks selge, milliseid meetmeid peaksid nii veebimajutusteenuse pakkujad kui ka pädevad asutused terroristliku veebisisu levitamise tõkestamiseks võtma, tuleks käesolevas määruses ennetavalt määratleda terroristlik sisu, lähtudes Euroopa Parlamendi ja nõukogu direktiivis (EL) 2017/541[4] kasutatud terroriakti määratlusest. Arvestades, et tegeleda tuleb kõige kahjulikuma internetis esineva terroristliku propagandaga, peaks määratlus hõlmama materjale [...], mis õhutavad, julgustavad või toetavad terroriaktide toimepanemist või neile kaasaaitamist või [...] propageerivad osalemist terrorirühmituse tegevuses. [...] ***Määratlus hõlmab sisu, mis annab suuniseid lõhkeainete, tulirelvade või muude relvade või kahjulike või ohtlike ainete, samuti KBRT-ainete valmistamise ja kasutamise kohta, või muude meetodite või tehnikate kohta, sealhulgas sihtmärkide valimise kohta terroriaktide toimepanemise eesmärgil.*** Selline [...] ***materjal*** hõlmab eelkõige teksti, kujutisi, helisalvestisi ja videoid. Kui pädevad asutused või veebimajutusteenuse pakkujad analüüsivad, kas sisu on käesoleva määruse tähenduses terroristlik, peaksid nad arvesse võtma selliseid aspekte nagu väidete laad ja sõnastus, nende esitamise kontekst ja tõenäosus, et neil on kahjulikud tagajärjed, mis mõjutavad inimeste turvalisust ja ohutust. Oluline tegur, mida hindamisel arvesse võtta, on see, kui materjali on koostanud ELi terroriorganisatsioonide või terroristide nimekirja kuuluv isik, selle võib talle omistada või seda levitatakse tema nimel. Sisu levitamist hariduslikul, [...] ***vastupropaganda*** või teaduslikul eesmärgil tuleks asjakohaselt kaitsta, ***leides õiglase tasakaalu põhiõiguste, sealhulgas eelkõige sõna- ja teabevajaduse ning avaliku julgeoleku vajaduste vahel. Kui materjal avaldatakse sisuteenuse osutaja toimetusvastutuse kohaselt, peab sellise sisu eemaldamise igasuguse otsuse puhul võtma arvesse ajakirjandus- ja meediavabaduse määruses kehtestatud ajakirjandusstandardeid, kooskõlas liidu õigusega ja põhiõiguste harta artiklis 11 sätestatud õigusega väljendusvabadusele ning meedia mitmekesisusele ja vabadusele.*** Terroristlikuks sisuks ei tohiks pidada radikaalsete, poleemiliste või vastuoluliste seisukohtade väljendamist tundlike poliitiliste küsimuste üle peetavas avalikus mõttevahetuses.

---

[4] 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).

(10) Et hõlmatud saaksid ka need veebimajutusteenused, mille kaudu terroristlikku sisu levitatakse, tuleks käesolevat määrust kohaldada infoühiskonna teenuste suhtes, mille puhul teenuse kasutaja antud teavet ***ja materjale*** talletatakse tema palvel ning talletatud teave ***ja materjal*** tehakse kättesaadavaks kolmandatele isikutele, olenemata sellest, kas selline tegevus on oma olemuselt puhtalt tehniline, automaatne või passiivne. [...] ***Sisu talletamine tähendab andmete hoidmist füüsilise või virtuaalse serveri mälus; see välistab teabe pelga edastamise ja muud elektroonilise side teenused [Euroopa elektroonilise side seadustiku] tähenduses või vahemäluteenuse osutajad või muud teenused, mida osutatakse interneti infrastruktuuri muudes kihtides, näiteks registrid ja registripidajad, domeeninimede süsteemid või sellega külgnevad teenused, nagu makseteenuste või hajusa teenusetõkestuse kaitse teenused. Lisaks peab teabe talletamine toimuma sisuteenuse pakkuja palvel; kohaldamisalasse kuuluvad ainult sellised teenused, mille puhul sisuteenuse pakkuja on otsene teenusesaaja. Lõpuks tehakse talletatud teave kättesaadavaks kolmandatele osapooltele, kusjuures peetakse silmas mis tahes kolmandat kasutajat, kes ei ole sisuteenuse pakkuja. Kohaldamisalasse ei kuulu isikutevahelise side teenus, mis võimaldab isikutevahelist otsest ja interaktiivset teabevahetust lõpliku arvu isikute vahel ning mille puhul side algatanud või selles osalevad isikud määravad kindlaks teabe saaja(d).*** Selliste ***veebimajutusteenuse*** pakkujate [...] hulka kuuluvad näiteks sotsiaalmeediaplatvormid, videovoogedastuse teenused, video-, pildi- ja audiomaterjalide jagamise teenused, failivahetus- ja muud pilvteenused ***ning salvestus***teenused [...]. ***Käesolevat määrust kohaldatakse veebimajutusteenuse pakkumise tegevuse, mitte niivõrd konkreetse teenusepakkuja või tema peamise tegevuse suhtes, milles majutusteenus võib olla kombineeritud muude teenustega, mis käesoleva määruse kohaldamisalasse ei kuulu.***

(10a) Määrust tuleks kohaldada ka nende veebimajutusteenuse pakkujate suhtes, kelle tegevuskoht on väljaspool liitu, kuid kes pakuvad siin teenuseid, sest suur osa veebimajutusteenuse pakkujaid, kes oma teenuseid pakkudes puutuvad kokku terroristliku sisuga, tegutsevad kolmandates riikides. See peaks tagama, et kõik digitaalsel ühtsel turul tegutsevad ettevõtjad järgivad samu nõudeid olenemata sellest, millises riigis on nende tegevuskoht. Selleks et kindlaks teha, kas teenuse pakkuja pakub teenuseid liidus, tuleb hinnata, kas teenuse pakkuja võimaldab juriidilistel või füüsilistel isikutel kasutada oma teenuseid ühes või mitmes liikmesriigis. Üksnes asjaolu, et teenusepakkuja veebisait või e-posti aadress või muud kontaktandmed on kättesaadavad ühes või mitmes liikmesriigis, ei ole eraldivõetuna käesoleva määruse kohaldamiseks piisav tingimus.

(11) Käesoleva määruse kohaldamisala kindlaksmääramisel tuleks lähtuda sellest, kas esineb sisuline seos liiduga. Niisugune sisuline seos on olemas, kui teenusepakkujal on liidus tegevuskoht, või kui seda ei ole, märkimisväärne arv kasutajaid ühes või mitmes liikmesriigis või tema tegevus on suunatud ühte või mitmesse liikmesriiki. Tegevuse suunatuse ühte või mitmesse liikmesriiki saab kindlaks teha kõigi asjakohaste asjaolude alusel, mille hulka kuuluvad sellised tegurid nagu selles liikmesriigis üldiselt kasutatava keele või vääringu kasutamine või kaupade või teenuste tellimise võimalus. Seda, kas tegevus on suunatud konkreetsesse liikmesriiki, saab järeldada ka rakenduse kättesaadavusest selle riigi rakendustepoes, kohaliku reklaami või selles liikmesriigis räägitavas keeles reklaami pakkumisest või kliendisuhete haldamisest, näiteks klienditeenuse pakkumisest selles liikmesriigis üldiselt kasutatavas keeles. Sisulise seose olemasolu tuleks eeldada ka siis, kui teenusepakkuja suunab oma tegevuse ühte või mitmesse liikmesriiki Euroopa Parlamendi ja nõukogu määruse 1215/2012[5] artikli 17 lõike 1 punkti c tähenduses. Teisalt, kui teenust osutatakse lihtsalt selleks, et järgida Euroopa Parlamendi ja nõukogu määruses (EL) 2018/302[6] sätestatud diskrimineerimiskeeldu, ei saa seda üksnes kõnealusele asjaolule tuginedes käsitada tegevuse suunamisena teatavale territooriumile liidus.

---

[5] 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).

[6] 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 601, 2.3.2018, lk 1).

(12) Veebimajutusteenuse pakkujad peaksid täitma teatavat hoolsuskohustust, et tõkestada terroristliku sisu levitamist oma teenuste kaudu. Selline hoolsuskohustus ei tohiks tähendada üldist jälgimiskohustust. Käesoleva määruse kohaldamisel peaks hoolsuskohustus hõlmama seda, et veebimajutusteenuse pakkuja tegutseb enda talletatava sisu suhtes hoolikalt, proportsionaalselt ja mittediskrimineerivalt, eeskätt oma tingimusi rakendades, et vältida sellise sisu eemaldamist, mis ei ole terroristlik ***sisu***. Sisu eemaldamisel ja juurdepääsu blokeerimisel tuleb austada sõna- ja teabevabadust.

(13) Ühtlustada tuleks menetlused ja kohustused, mis tulenevad õigusekohaselt tehtud korraldusest, mille kohaselt peaks veebimajutusteenuse pakkuja eemaldama terroristliku sisu või blokeerima juurdepääsu sellele pärast pädeva asutuse hindamist. Liikmesriikidele peaks jääma vabadus selline pädev asutus ise valida, et nad saaksid määrata kõnealuse ülesandega tegelema haldus-, õiguskaitse- või kohtuasutuse. Arvestades, kui kiiresti levib terroristlik sisu internetipõhiste teenuste vahel, kohustab käesolev säte veebimajutusteenuse osutajaid tagama, et eemaldamiskorralduses kirjeldatud terroristlik sisu eemaldatakse või juurdepääs sellele blokeeritakse ühe tunni jooksul alates eemaldamiskorralduse kättesaamisest. ***Ilma et see piiraks käesoleva määruse artiklis 7 või elektroonilisi tõendeid käsitleva direktiivi eelnõus sätestatud andmete säilitamise nõuet***, otsustab veebimajutusteenuse pakkuja ise, kas eemaldab kõnealuse sisu või blokeerib liidu kasutajate juurdepääsu sellele sisule. ***See peaks takistama juurdepääsu või vähemalt muutma selle keeruliselt teostatavaks ning tõsiselt raskendama nende teenuseid tarbivate internetikasutajate juurdepääsu sisule, millele juurdepääs on blokeeritud.***

(13a) Eemaldamiskorraldus peaks sisaldama asjaomase sisu klassifitseerimist terroristlikuks sisuks ning piisavat teavet võimaldamaks määrata kindlaks sisu asukoht, esitades selleks URLi ja mis tahes täiendava teabe, näiteks kuvatõmmise asjaomasest sisust. Taotluse korral peaks pädev asutus esitama täiendavad põhjendused selle kohta, miks kõnealust sisu peetakse terroristlikuks sisuks. Esitatud põhjendused ei pea sisaldama tundlikku teavet, mis võiks uurimist kahjustada. Põhjendused peaksid siiski võimaldama veebimajutusteenuse pakkujal ja lõpuks sisuteenuse pakkujal kasutada tõhusalt oma õigust õiguskaitsele.

(14) Pädev asutus peaks edastama eemaldamiskorralduse otse adressaadile ja kontaktpunktile mis tahes elektroonilisel kujul, mille kohta jääb maha kirjalik jälg, tingimustel, mis võimaldavad teenusepakkujal teha kindlaks korralduse autentsuse, kaasa arvatud selle saatmise ja kättesaamise täpse kuupäeva ja kellaaja; selleks kasutatakse näiteks turvalisi e-kirju ja platvorme või muid turvalisi kanaleid, mille hulka kuuluvad ka need, mille on teinud kättesaadavaks teenusepakkuja, kooskõlas isikuandmete kaitse õigusnormidega. Selle nõude täitmiseks võib kasutada kvalifitseeritud e-andmevahetusteenuseid vastavalt Euroopa Parlamendi ja nõukogu määrusele (EL) 910/2014[7].

[7] 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).

(15) [...] [...] ***Esildiste*** mehhanism, mis võimaldab juhtida veebimajutusteenuse pakkuja tähelepanu teabele ***ja materjalile***, mida võib pidada terroristlikuks sisuks, et teenusepakkuja saaks vabatahtlikult kaaluda selle sisu vastavust oma tingimustele, [...]***on eriti tulemuslik, kiire ja proportsionaalne vahend, millega saab veebimajutusteenuse pakkujale teada anda tema teenuse konkreetsest sisust*** [...]. On oluline, et veebimajutusteenuse pakkujad hindaksid selliseid esildisi esmajärjekorras ja annaksid võetud meetmete kohta kiirelt tagasisidet. Lõpliku otsuse selle kohta, kas sisu eemaldada tingimustele mittevastavuse tõttu, teeb veebimajutusteenuse pakkuja. Kui käesolevat määrust rakendatakse esildiste suhtes, ei mõjuta see määruses (EL) 2016/794[8] sätestatud Europoli volitusi.

(16) Arvestades, kui ulatuslikult ja kiiresti tuleb terroristliku sisu kindlakstegemiseks ja eemaldamiseks tegutseda, on proportsionaalsed ennetavad meetmed, teatavatel juhtudel muu hulgas ka automaatsete vahendite kasutamine, terroristliku veebisisu vastu võitlemises olulisel kohal. Et vähendada terroristlikule sisule juurdepääsetavust oma teenuste kaudu, peaksid veebimajutusteenuse pakkujad hindama ennetavate meetmete võtmise otstarbekust, lähtudes terroristliku sisuga kokkupuutumise riskidest ja ulatusest ning sellest, millist mõju see avaldab kolmandate isikute õigustele ja üldsuse huvile olla informeeritud. Seega peaksid veebimajutusteenuse pakkujad kindlaks tegema, millised asjakohased, mõjusad ja proportsionaalsed ennetavad meetmed tuleks kehtestada. See nõue ei tohiks tähendada üldist jälgimiskohustust. Sellise hindamise puhul annab veebimajutusteenuse pakkujale adresseeritud eemaldamiskorralduste ja esildiste puudumine märku sellest, et ***risk või*** kokkupuude terroristliku sisuga on vähene.

---

8 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).

(17) Ennetavate meetmete kehtestamisel peaks veebimajutusteenuse pakkuja tagama, et säilib kasutajate õigus sõna- ja teabevabadusele, kaasa arvatud õigus vabalt saada ja anda teavet. Lisaks selliste õigusest tulenevate nõuete järgimisele, mis on ette nähtud muu hulgas isikuandmete kaitset käsitletavate õigusaktidega, peaksid veebimajutusteenuse pakkujad tegutsema nõuetekohase hoolsusega ja rakendama vajaduse korral kaitsemeetmeid, sh eeskätt inimeste teostatavat jälgimist ja kontrollimist, et vältida tahtmatuid ja ekslikke otsuseid, mille tulemusena eemaldataks sisu, mis ei ole terroristlik. See on eriti oluline juhul, kui veebimajutusteenuse pakkujad kasutavad terroristliku sisu avastamiseks automaatseid vahendeid. Olenemata sellest, kas otsuse kasutada automaatseid vahendeid teeb veebimajutusteenuse pakkuja omal algatusel või lähtudes pädeva asutuse taotlusest, tuleks sellist otsust hinnata lähtuvalt kasutatavast tehnoloogiast ja põhiõigustele avaldatavast mõjust.

(18) Tagamaks, et terroristliku sisuga kokku puutunud veebimajutusteenuse pakkuja võtab asjakohaseid meetmeid, et tõkestada oma teenuste kuritarvitamist, peaksid pädevad asutused nõudma, et lõplikuks muutunud eemaldamiskorralduse saanud veebimajutusteenuse pakkuja annaks aru võetud ennetavate meetmete kohta. Ennetavateks meetmeteks võivad olla meetmed, millega tõkestatakse sellise terroristliku sisu uuesti üleslaadimist, mis on eemaldamiskorralduse või esildise põhjal juba eemaldatud või millele juurdepääs on blokeeritud, ning sisu võrdlemine avalik-õiguslike või eraõiguslike vahenditega, mis sisaldavad teadaolevalt terroristlikku sisu. Nende jaoks võidakse kasutada usaldusväärseid (kas turul olevaid või veebimajutusteenuse pakkuja enda arendatud) tehnilisi vahendeid, mille abil uut terroristlikku sisu kindlaks teha. Teenusepakkuja peaks andma aru konkreetsete kehtestatud ennetavate meetmete kohta, et pädev asutus saaks hinnata nende meetmete mõjusust ja proportsionaalsust ning juhul, kui kasutatakse automaatseid vahendeid, ka seda, kas veebimajutusteenuse pakkujal on inimeste teostatava jälgimise ja kontrollimise suutlikkus. Meetmete mõjususe ja proportsionaalsuse hindamisel peaksid pädevad asutused võtma arvesse asjaomaseid parameetreid, sealhulgas teenusepakkujale tehtud eemaldamiskorralduste ja esildiste arvu, tema majanduslikku suutlikkust ja tema teenuse mõju terroristliku sisu levitamisele (võttes arvesse näiteks liidus olevate kasutajate arvu).

(19) Vastavasisulise taotluse peale peaks pädev asutus alustama veebimajutusteenuse pakkujaga dialoogi kehtestamist vajavate ennetavate meetmete üle. Kui pädev asutus leiab, et võetud meetmed ei ole riskide katmiseks piisavad, peaks ta vajaduse korral kehtestama kohustuse võtta asjakohaseid, mõjusaid ja proportsionaalseid ennetavaid meetmeid. Põhimõtteliselt ei tohiks selliste ennetavate meetmete kehtestamise otsus viia üldise jälgimiskohustuse kehtestamiseni vastavalt direktiivi 2000/31/EÜ artikli 15 lõikele 1. Võttes arvesse terroristliku sisu levikuga seotud eriti suuri riske, võib pädevate asutuste käesoleva määruse alusel vastu võetud otsuste puhul teha erandeid direktiivi 2000/31/EÜ artikli 15 lõikes 1 sätestatud lähenemisviisist selles osas, mis puudutab teatavaid konkreetseid sihipäraseid meetmeid, mille vastuvõtmine on vajalik avaliku julgeolekuga seotud ülekaalukatel põhjustel. Enne sellise otsuse vastuvõtmist peaks pädev asutus leidma õiglase tasakaalu avaliku huvi eesmärkide ning asjassepuutuvate põhiõiguste vahel (eriti seoses sõna- ja teabevabaduse ja ettevõtlusvabadusega) ning seda asjakohaselt põhjendama.

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

(21) Kohustus säilitada sisu halduslikus või kohtulikus korras toimuva kontrollimise jaoks on vajalik ja põhjendatud selleks, et tagada tulemuslikud õiguskaitsevahendid sisuteenuse pakkujale, kelle sisu eemaldati või kelle sisule juurdepääs blokeeriti, ning tagada selle sisu taastamine samasugusena, nagu see oli enne eemaldamist, vastavalt läbivaatamise tulemustele. Kohustus säilitada sisu uurimise või süüdistuse esitamisega seotud eesmärgil on põhjendatud ja vajalik, arvestades kõnealuse materjali väärtust terrorismi nurjamisel ja tõkestamisel. Kui ettevõtja eemaldab materjali või blokeerib juurdepääsu sellele eeskätt oma ennetavate meetmete abil ega teata sellest asjaomasele ametiasutusele, sest tema hinnangul ei kuulu see käesoleva määruse artikli 13 lõike 4 kohaldamisalasse, ei pruugi õiguskaitseorganid sellise sisu olemasolust teadlikud olla. Seepärast on põhjendatud ka sisu säilitamine terroriaktide tõkestamise, avastamise, uurimise ja nende eest süüdistuse esitamise eesmärgil. Nimetatud eesmärkidel andmete säilitamise nõue piirdub andmetega, millel on tõenäoliselt seos terroriaktidega ja mis võivad seega aidata esitada süüdistust terroriakti eest või hoida ära tõsiseid avalikku julgeolekut ähvardavaid riske.

(22) Proportsionaalsuse tagamise huvides tuleks säilitamisaja pikkuseks määrata kuni kuus kuud, et sisuteenuse pakkujale jääks piisavalt aega, et algatada läbivaatamine, ja et õiguskaitseasutustel oleks võimalus pääseda juurde terroriaktide uurimise ja nende eest süüdistuse esitamise seisukohast olulistele andmetele. Kui läbivaatamine küll algatatakse kuue kuu jooksul, kuid seda ei viida lõpule, võib seda ajavahemikku läbivaatamist teostava ametiasutuse taotlusel pikendada nii kauaks kui vaja. See ajavahemik peaks olema piisav, et õiguskaitseasutused saaksid uurimistega seotud vajalikud tõendid säilitada, tagades ühtlasi tasakaalu asjaomaste põhiõigustega.

(23) Käesolev määrus ei mõjuta menetluslikke tagatisi ja uurimismeetmeid, mis on seotud juurdepääsuga infosisule ja seotud andmetele, mida säilitatakse terroriaktide uurimise ja nende eest süüdistuse esitamise eesmärgil vastavalt liikmesriikide õigusele ja liidu õigusele.

(24) Veebimajutusteenuse pakkujate terroristlikku sisu käsitlevate põhimõtete läbipaistvus on äärmiselt tähtis, et parandada nende vastutust kasutajate ees ja suurendada kodanike usaldust digitaalse ühtse turu vastu. Veebimajutusteenuse pakkujad, kellel on ***kokkupuude terroristliku sisuga***, peaksid igal aastal avaldama läbipaistvusaruande, mis sisaldab sisulist teavet terroristliku sisu avastamiseks, kindlakstegemiseks ja eemaldamiseks võetud meetmete kohta, ***kui see ei ole vastuolus võetud meetmete eesmärkidega.***

(25) Kaebuste lahendamise menetlused on vajalik kaitsemeede sõna- ja teabevabadusega kaitstud infosisu eksliku kõrvaldamise eest ***veebimajutusteenuse pakkuja tingimustest tulenevalt võetud meetmete tulemusel***. 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, ei mõjuta veebimajutusteenuse pakkuja võimalust tagada oma tingimuste täitmine muudel alustel. ***Lisaks peaks sisuteenuse pakkujatel, kelle sisu on eemaldamiskorralduse alusel eemaldatud, olema Euroopa Liidu lepingu artikli 19 ja Euroopa Liidu põhiõiguste harta artikli 47 kohane õigus tõhusale õiguskaitsele.***

(26) ***Üldisemalt*** eeldab Euroopa Liidu lepingu artikli 19 ja Euroopa Liidu põhiõiguste harta artikli 47 kohane tõhus õiguskaitse, et isikud saavad tutvuda põhjendustega, mille alusel nende üleslaaditud sisu on eemaldatud või juurdepääs sellele blokeeritud. Sellel eesmärgil peaks veebimajutusteenuse pakkuja tegema sisuteenuse pakkujale kättesaadavaks sisulise teabe, et sisuteenuse pakkujal oleks võimalik otsus vaidlustada. Selleks ei ole ilmtingimata vaja sisuteenuse pakkujale teadet saata. Olenevalt asjaoludest võib majutusteenuse pakkuja asendada terroristlikuks peetava sisu sõnumiga selle kohta, et sisu on eemaldatud või juurdepääs sellele blokeeritud kooskõlas käesoleva määrusega. Täiendavat teavet põhjuste, aga ka sisuteenuse pakkuja võimaluste kohta see otsus vaidlustada tuleks anda vastavasisulise taotluse korral. Kui pädevad asutused otsustavad, et avaliku julgeolekuga seotud põhjustel, kaasa arvatud seoses uurimisega, oleks sisu eemaldamise või sellele juurdepääsu blokeerimise kohta käiva teabe esitamine otse sisuteenuse pakkujale sobimatu või kahjulik, peaksid nad teavitama veebimajutusteenuse pakkujat.

(27) […] ***Enne*** kui pädevad asutused teevad veebimajutusteenuse pakkujatele eemaldamiskorraldusi või ***siis***, kui nad saadavad esildisi, peaksid nad jagama teavet, koordineerima ja tegema koostööd omavahel ja vajaduse korral ka Europoliga, et vältida topelttööd ja võimalikku sekkumist uurimistesse („dekonfliktimine“). […] ***Eemaldamiskorralduse otsust tehes peaks pädev asutus võtma nõuetekohaselt arvesse mis tahes teateid uurimistesse sekkumiste kohta („dekonfliktimine“). Kui ühe liikmesriigi pädev asutus teavitab teise liikmesriigi pädevat asutust kehtivast eemaldamiskorraldusest, siis dubleerivat korraldust välja anda ei ole vaja.*** Käesoleva määruse sätete rakendamisel võiks Europol pakkuda toetust kooskõlas oma praeguste volituste ja kehtiva õigusraamistikuga.

(28) Ennetavate meetmete tulemusliku ja piisavalt sidusa rakendamise tagamiseks peaksid liikmesriikide pädevad asutused jagama üksteisega teavet arutelude kohta, mida nad peavad veebimajutusteenuse pakkujatega konkreetsete ennetavate meetmete kindlaksmääramise, rakendamise ja hindamise üle. Samalaadset koostööd tuleb teha ka karistusi käsitlevate õigusnormide vastuvõtmise ning karistuste rakendamise ja nende täitmise tagamise vallas. ***Komisjon peaks sellist koordineerimist ja koostööd hõlbustama.***

(29) On äärmiselt oluline, et karistuste kehtestamise eest vastutava liikmesriigi pädev asutus oleks täielikult teadlik eemaldamiskorralduste ja esildiste tegemisest ja sellele järgnevast teabevahetusest veebimajutusteenuse pakkuja ja asjaomase pädeva asutuse vahel. Selle eesmärgi saavutamiseks peaksid liikmesriigid tagama asjakohaste sidekanalite ja -mehhanismide olemasolu, et nende kaudu saaks asjakohast teavet õigeaegselt jagada.

(30) Hõlbustamaks sujuvat teabevahetust pädevate asutuste vahel, aga ka veebimajutusteenuse pakkujatega, ning vältimaks topelttööd, [...] ***soovitatakse*** liikmesriikidel kasutada Europoli välja töötatud ***asjaomaseid*** vahendeid, näiteks praegu kasutusel olevat veebisisust teavitamise haldamise rakendust (IRMa) või tulevasi vahendeid.

(31) Arvestades, et teatava terroristliku sisu tagajärjed võivad olla eriti tõsised, peaks veebimajutusteenuse pakkuja viivitamata teavitama asjaomase liikmesriigi ametiasutusi või selle riigi pädevaid asutusi, kus ta asub või kus tal on esindaja, kui temani jõuab teave terroriakti kohta käivast tõendusmaterjalist. 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 selliseid tõendusmaterjale aktiivselt otsida. Asjaomane liikmesriik on liikmesriik, kelle jurisdiktsiooni alla terroriaktide uurimine ja nende eest süüdistuse esitamine kuulub vastavalt direktiivile (EL) 2017/541, lähtudes õigusrikkuja või õigusrikkumise võimaliku ohvri kodakondsusest või terroriakti sihtkohast. Kahtluse korral võib veebimajutusteenuse pakkuja edastada teabe Europolile, kes peaks võtma edasisi meetmeid vastavalt oma volitustele ning muu hulgas edastama teabe liikmesriikide asjaomastele ametiasutustele.

(32) Liikmesriikide pädevatel asutustel peaks olema lubatud kasutada sellist teavet liikmesriigi või liidu õiguse kohaste uurimistoimingute jaoks, kaasa arvatud Euroopa andmeesitamismääruse tegemiseks vastavalt määrusele, mis käsitleb Euroopa andmeesitamismäärust ja Euroopa andmesäilitamismäärust elektrooniliste tõendite hankimiseks kriminaalasjades[9].

(33) Nii veebimajutusteenuse pakkujad kui ka liikmesriigid peaksid looma kontaktpunktid, et hõlbustada eemaldamiskorralduste ja esildiste kiiret menetlemist. Erinevalt esindajast täidab kontaktpunkt korralduslikke eesmärke. Veebimajutusteenuse pakkuja kontaktpunkti peaksid moodustama mis tahes sihtotstarbelised ***asutusesisesed või lepingulised*** vahendid, mille abil saab elektrooniliselt esitada eemaldamiskorraldusi ja esildisi, ning nende kiireks töötlemiseks vajalikud tehnilised vahendid [...] ***või*** inimressursid. Veebimajutusteenuse pakkuja kontaktpunkt ei pea asuma liidus ning veebimajutusteenuse pakkujal on vabadus nimetada mõni olemasolev kontaktpunkt, kui see suudab täita käesolevas määruses sätestatud ülesandeid. Selleks, et terroristlik sisu eemaldataks või juurdepääs sellele blokeeritaks ühe tunni jooksul pärast eemaldamiskorralduse saamist, peab ***terroristliku sisuga kokku puutunud (sellest annab tunnistust eemaldamiskorralduse saamine) veebimajutusteenuse pakkuja*** tagama, et kontaktpunkt on kättesaadav seitse päeva nädalas ööpäev läbi. 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 ametlikest keeltest, milles on kättesaadavad nende teenuse tingimused.

(34) Kuna puudub üldine nõue, et teenusepakkujad peavad tagama füüsilise kohalviibimise liidu territooriumil, tuleb 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 määratud esindaja. ***Siiski peaks tõhusa rakendamise, küsimuse kiireloomulisuse ja avaliku korra huvides olema liikmesriikidel pädevus eemaldamiskorralduste ja esildiste suhtes***.

---

9 COM(2018) 225 (lõplik).

(35) Veebimajutusteenuse pakkuja, kelle tegevuskoht ei ole liidus, peaks määrama kirjalikus vormis esindaja, et tagada käesoleva määruse järgimine ja sellest tulenevate kohustuste täitmine. ***Veebimajutusteenuse pakkuja võib kasutada olemasolevat esindajat tingimusel, et kõnealune esindaja suudab täita käesolevas määruses sätestatud funktsioone.***

(36) Esindaja peaks olema seaduslikult volitatud tegutsema veebimajutusteenuse pakkuja nimel.

(37) Liikmesriigid peaksid määrama käesoleva määruse kohaldamiseks pädevad asutused. Pädeva asutuse määramise nõue ei eelda tingimata uute asutuste loomist; tegemist võib olla olemasolevate asutustega, kellele pannakse käesolevas määruses sätestatud ülesanded. Käesoleva määruse kohaselt tuleb määrata ametiasutus, kes oleks pädev tegema eemaldamiskorraldusi ja esildisi, jälgima ennetavaid meetmeid ja määrama karistusi. Liikmesriigid ise otsustavad, kui mitu asutust nad tahavad nende ülesannetega tegelema määrata.

(38) Karistused on vajalikud, et tagada käesoleva määruse kohaste kohustuste tulemuslik täitmine veebimajutusteenuse pakkuja poolt. Liikmesriigid peaksid kehtestama õigusnormid karistuste kohta, ***mis võivad olla haldus- või kriminaalkaristused***, ning vajaduse korral trahvimissuunised. Eriti ranged karistused määratakse juhul, kui veebimajutusteenuse pakkuja jätab süstemaatiliselt terroristliku sisu eemaldamata või ei blokeeri juurdepääsu sellele ühe tunni jooksul pärast eemaldamiskorralduse kättesaamist. Kui nõudeid rikutakse üksikjuhtudel, võidakse nende eest karistada, järgides topeltkaristamise keeldu ja proportsionaalsuse põhimõtet ning tagades, et selliste karistuste puhul võetakse arvesse süstemaatilist korralduste täitmata jätmist. Õiguskindluse tagamiseks tuleks määruses sätestada, millises ulatuses võib asjaomaste kohustuste puhul karistusi rakendada. Artikli 6 nõuete rikkumise eest tuleks karistusi kehtestada üksnes siis, kui kohustus tuleneb artikli 6 lõikes 2 sätestatud nõudest esitada aruandeid või otsusest kehtestada täiendavad ennetavad meetmed vastavalt artikli 6 lõikele 4. ***Rikkumise olemuse hindamisel ja karistuste kohaldamise üle otsustamisel tuleks täiel määral arvesse võtta põhiõigusi, nagu väljendusvabadus.*** Kui otsustatakse, kas kehtestada rahaline karistus, tuleks nõuetekohaselt arvesse võtta teenusepakkuja finantsvahendeid. Liikmesriigid tagavad, et karistused ei õhutaks eemaldama sisu, mis ei ole terroristlik.

(39) Standardvormide kasutamine hõlbustab koostööd ja teabevahetust pädevate asutuste ja teenusepakkujate vahel ning võimaldab neil suhelda kiiremini ja tulemuslikumalt. Eriti oluline on tagada kiire tegutsemine pärast eemaldamiskorralduse kättesaamist. Vormide kasutamine vähendab tõlkekulusid ja edendab teabevahetuse kvaliteeti. Sama moodi peaksid standarditud teabevahetust toetama vastusevormid; nende kasutamine on eriti oluline juhul, kui teenusepakkuja ei suuda nõudeid täita. Autenditud edastuskanalid võivad tagada eemaldamiskorralduse autentsuse, kaasa arvatud korralduse saatmise ja vastuvõtmise kuupäeva ja kellaaja täpsuse.

(40) Et käesoleva määruse kohaldamisel kasutatavate vormide sisu saaks vajaduse korral sujuvalt muuta, tuleks komisjonile anda Euroopa Liidu toimimise lepingu artikli 290 kohane õigus võtta vastu õigusakte käesoleva määruse I, II ja III lisa 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 toimuksid kooskõlas 13. aprilli 2016. aasta institutsioonidevahelises parema õigusloome kokkuleppes[10] 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.

(41) Liikmesriigid peaksid koguma teavet õigusaktide rakendamise kohta. ***Liikmesriigid võivad kasutada veebimajutusteenuse pakkujate läbipaistvuse aruandeid ja esitada vajaduse korral täienduseks üksikasjalikumat teavet.*** Käesoleva määruse väljundite, tulemuste ja mõju jälgimiseks tuleks koostada üksikasjalik programm, millest lähtudes õigusakti hinnata.

10 ELT L 123, 12.5.2016, lk 1.

(42) Komisjon peaks hindama käesolevat määrust mitte varem kui kolm aastat pärast selle jõustumist, lähtudes rakendamisaruande tähelepanekutest ja järeldustest ning jälgimistulemustest. Hindamisel tuleks lähtuda viiest kriteeriumist: tõhusus, mõjusus, asjakohasus, sidusus ja ELi lisaväärtus. Hinnata tuleb mitmesuguste määruse kohaselt ettenähtud korralduslike ja tehniliste meetmete toimimist, sealhulgas selliste meetmete mõjusust, mille eesmärk on parandada terroristliku sisu avastamist, kindlakstegemist ja eemaldamist, kaitsemehhanismide mõjusust ning võimalikku mõju kolmandate isikute õigustele ja huvidele; muu hulgas vaadatakse läbi nõue teavitada sisuteenuse pakkujaid.

(43) Käesoleva määruse eesmärki – tagada digitaalse ühtse turu sujuv toimimine terroristliku veebisisu levitamise tõkestamise kaudu – ei saa piisavalt saavutada liikmesriikide tasandil ning selle piirangu ulatuse ja mõju tõttu on seda parem saavutada liidu tasandil; seega võib liit võtta vastu meetmeid kooskõlas Euroopa Liidu 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 sätestatakse ühtsed õigusnormid, et tõkestada veebimajutusteenuste kuritarvitamist terroristliku veebisisu levitamiseks. Täpsemalt sätestatakse määruses:

   a) õigusnormid, mis käsitlevad veebimajutusteenuse pakkujate hoolsuskohustust, et tõkestada terroristliku sisu levitamist oma teenuste kaudu ja tagada vajaduse korral sellise sisu kiire eemaldamine;

   b) meetmed, mille liikmesriigid peavad kehtestama, et teha kindlaks terroristlik sisu, teha võimalikuks selle kiire eemaldamine veebimajutusteenuste pakkujate poolt ning hõlbustada koostööd teiste liikmesriikide pädevate asutuste, veebimajutusteenuste pakkujate ja vajaduse korral ka asjaomaste liidu tasandi asutustega.

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

3. ***Käesolev määrus ei mõjuta kohustust austada põhiõigusi ja õiguse üldpõhimõtteid, nagu on sätestatud Euroopa Liidu lepingu artiklis 6.***

Artikkel 2

Mõisted

Käesolevas määruses kasutatakse järgmisi mõisteid:

1) „veebimajutusteenuse pakkuja“ – isik, kes pakub infoühiskonna teenuseid, mis seisnevad sisuteenuse pakkuja antud teabe talletamises sisuteenuse pakkuja soovil ning talletatud teabe kolmandatele isikutele kättesaadavaks tegemises;

2) „sisuteenuse pakkuja“ – kasutaja, kes on andnud teabe, mida veebimajutusteenuse pakkuja tema soovil talletab või on talletanud;

3) „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, näiteks veebimajutusteenuse pakkuja tegevuskoht on liidus;

Kui sellist tegevuskohta ei ole, hinnatakse olulist seost konkreetsete faktiliste kriteeriumide alusel, näiteks:

a) ühes või mitmes liikmesriigis on märkimisväärne arv kasutajaid;

b) ***või*** tegevus on suunatud ühele või mitmele liikmesriigile;

4) „terroriakt“ – ***üks*** direktiivi (EL) 2017/541 artikli 3 lõikes 1 [...] ***loetletud tahtlikest tegudest***;

5) „terroristlik sisu“ – [...] materjal, ***mis võib aidata kaasa direktiivi 2017/541 artikli 3 lõike 1 punktides a–i loetletud tahtlike tegude korraldamisele järgmisel viisil:***

aa) ähvardab korraldada terroriakti;

a) õhutab või õigustab, [...] ***näiteks*** [...] ***ülistab terroriakte***, terroriaktide sooritamist, põhjustades seega selliste aktide sooritamise ohu;

b) ***ärgitab isikuid või isikute rühmi korraldama*** [...] terroriakte või nendele kaasa aitama;

c) propageerib terrorirühmituse tegevust, eeskätt seeläbi, et ***ärgitab isikuid või isikute rühmi*** osalema direktiivi (EL) 2017/541 artikli 2 lõikes 3 määratletud terrorirühmituse ***kriminaalses tegevuses*** või sellist rühmitust toetama;

annab terroriaktide toimepanemise eesmärgil juhiseid meetodite või tehniliste võtete kohta;

6) „terroristliku sisu levitamine“ – terroristliku sisu kättesaadavaks tegemine kolmandatele isikutele veebimajutusteenuse pakkuja teenuste kaudu;

7) „tingimused“ – mis tahes nimetuse või vormiga kõikvõimalikud tingimused, mis reguleerivad veebimajutusteenuse pakkuja ja teenuse kasutajate lepingulist suhet;

8) „esildis“ – teade, mille pädev asutus või vajaduse korral asjaomane liidu asutus saadab veebimajutusteenuse pakkujale teabe kohta, mida võib pidada terroristlikuks sisuks, et teenusepakkuja saaks vabatahtlikult kaaluda selle sisu vastavust oma tingimustele, et seeläbi tõkestada terroristliku sisu levitamist;

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

II JAGU
TERRORISTLIKU VEEBISISU LEVITAMISE TÕKESTAMISE MEETMED

Artikkel 3

Hoolsuskohustus

1. Veebimajutusteenuse pakkujad võtavad vastavalt käesolevale määrusele asjakohaseid, mõistlikke ja proportsionaalseid meetmeid, et tõkestada terroristliku sisu levitamist ja kaitsta kasutajaid terroristliku sisu eest. Seejuures tegutsevad nad hoolsalt, proportsionaalselt ja mittediskrimineerivalt ning arvestavad nõuetekohaselt kasutajate põhiõigustega ja võtavad arvesse sõna- ja teabevabaduse olulisust avatud ja demokraatlikus ühiskonnas.

2. Veebimajutusteenuse pakkujad panevad oma tingimustesse kirja, ***et nad ei talleta terroristlikku veebisisu*** ning kohaldavad sätteid terroristliku sisu levitamise tõkestamise kohta.

Artikkel 4

Eemaldamiskorraldused

1. Pädeval asutusel on õigus anda välja [...] ***eemaldamiskorraldus***, millega kohustatakse veebimajutusteenuse pakkujat eemaldama terroristliku sisu või blokeerima juurdepääsu sellele.

2. Veebimajutusteenuse pakkuja eemaldab terroristliku sisu või blokeerib juurdepääsu sellele ühe tunni jooksul pärast eemaldamiskorralduse kättesaamist.

3. Eemaldamiskorraldus sisaldab järgmisi komponente vastavalt I lisas esitatud vormile:

   a) eemaldamiskorralduse teinud pädeva asutuse nimi ja eemaldamiskorralduse autentsuse kinnitamine pädeva asutuse poolt; […] ***sisu hindamine***, sealjuures viidatakse vähemalt artikli 2 lõikes 5 loetletud terroristliku sisu ***asjaomastele*** kategooriatele;

b) URL (ühtne ressursilokaator) ja vajaduse korral täiendav teave, mille põhjal saaks asjaomase sisu kindlaks teha;

c) viide käesolevale määrusele kui eemaldamiskorralduse õiguslikule alusele;

d) korralduse tegemise kuupäev ja ajatempel;

e) teave veebimajutusteenuse pakkujale ja sisuteenuse pakkujale kättesaadavate õiguskaitsevahendite kohta;

f) kui see on asjakohane, artiklis 11 osutatud otsus, et teavet terroristliku sisu eemaldamise või sellele juurdepääsu blokeerimise kohta ei avalikustata.

4. Veebimajutusteenuse pakkuja või sisuteenuse pakkuja taotluse peale esitab pädev asutus [...] ***täiendava*** põhjenduse, milles ***selgitatakse, miks peetakse asjaomast sisu terroristlikuks sisuks***, ilma et see piiraks veebimajutusteenuse pakkuja kohustust täita eemaldamiskorraldus lõikes 2 sätestatud tähtaja jooksul.

5. Pädevad asutused adresseerivad eemaldamiskorralduse veebimajutusteenuse pakkuja peamisesse tegevuskohta või esindajale, kelle veebimajutusteenuse pakkuja on määranud vastavalt artiklile 16, ning edastavad selle artikli 14 lõikes 1 osutatud kontaktpunkti. Korraldused saadetakse elektroonilisel kujul, mille kohta jääb maha kirjalik jälg, mis võimaldab saatja autentida, kaasa arvatud korralduse saatmise ja vastuvõtmise kuupäeva ja kellaaja täpsuse.

6. ***Ilma põhjendamatu viivituseta*** [...] kinnitab veebimajutusteenuse pakkuja korralduse kättesaamist ja […] teatab pädevale asutusele terroristliku sisu eemaldamisest või sellele juurdepääsu blokeerimisest ning märgib ära eeskätt tegevuse toimumise kellaaja, kasutades selleks II lisas esitatud vormi.

7. Kui veebimajutusteenuse pakkuja ei saa eemaldamiskorraldust täita vääramatu jõu tõttu või kuna see on veebimajutusteenuse pakkujast sõltumatutel põhjustel reaalselt võimatu, teatab ta sellest ilma põhjendamatu viivituseta pädevale asutusele ja esitab selgitused, kasutades selleks III lisas sätestatud vormi. Lõikes 2 sätestatud tähtaeg hakkab kehtima kohe, kui viidatud põhjuseid enam ei esine.

8. Kui veebimajutusteenuse pakkuja ei saa eemaldamiskorraldust täita, sest see sisaldab selgeid vigu või ei sisalda piisavalt teavet, et korralduse saaks täita, teatab ta sellest ilma põhjendamatu viivituseta pädevale asutusele ja küsib vajalikke selgitusi, kasutades selleks III lisas sätestatud vormi. Lõikes 2 sätestatud tähtaeg hakkab kehtima kohe, kui selgitused on esitatud.

9. Kui eemaldamiskorraldus muutub lõplikuks, teatab eemaldamiskorralduse teinud pädev asutus sellest artikli 17 lõike 1 punktis c osutatud pädevale asutusele, kes jälgib ennetavate meetmete rakendamist. Eemaldamiskorraldus muutub lõplikuks, kui seda ei ole tähtaja jooksul edasi kaevatud vastavalt kohaldatavale siseriiklikule õigusele või kui see on pärast edasikaebamist kinnitatud.

Artikkel 4a

Konsultatsioonimenetlus eemaldamiskorralduste jaoks

1. Eemaldamiskorralduse teinud pädev asutus esitab korralduse koopia artikli 17 lõike 1 punktis a osutatud pädevale asutusele selles liikmesriigis, kus on veebimajutusteenuse pakkuja peamine tegevuskoht, samal ajal, kui see kooskõlas artikli 4 lõikega 5 edastatakse veebimajutusteenuse pakkujale.

2. Kui selle liikmesriigi pädeval asutusel, kus on veebimajutusteenuse pakkuja peamine tegevuskoht, on piisavalt alust arvata, et eemaldamiskorraldus võib mõjutada kõnealuse liikmesriigi põhihuvisid, teavitab ta sellest korralduse teinud pädevat asutust.

3. Korralduse teinud asutus võtab neid asjaolusid arvesse ning vajaduse korral võtab korralduse tagasi või kohandab seda.

Artikkel 5

Esildised

1. Pädev asutus või asjaomane liidu asutus võib saata veebimajutusteenuse pakkujale esildise.

2. Veebimajutusteenuse pakkuja kehtestab korralduslikud ja tehnilised meetmed, mis hõlbustavad pädevate asutuste ja vajaduse korral liidu asjaomaste asutuste poolt neile vabatahtlikuks kaalumiseks saadetud sisu kiiret hindamist.

3. Esildis adresseeritakse veebimajutusteenuse pakkuja peamisesse tegevuskohta või esindajale, kelle teenusepakkuja on määranud vastavalt artiklile 16, ning edastatakse artikli 14 lõikes 1 osutatud kontaktpunkti. Esildised saadetakse elektrooniliselt.

4. Esildis peab sisaldama piisavat [...] teavet [...] põhjuste ***kohta***, miks sisu peetakse terroristlikuks ning ***esitab*** URLi ja vajaduse korral täiendava teabe, mille põhjal viidatud terroristlik sisu kindlaks teha.

5. Veebimajutusteenuse pakkuja hindab esildises kirjeldatud sisu esimesel võimalusel, võrdleb seda oma tingimustega ning otsustab, kas sisu tuleks eemaldada või blokeerida juurdepääs sellele.

6. Veebimajutusteenuse pakkuja teavitab pädevat asutust või asjaomast liidu asutust ***ilma põhjendamatu viivituseta*** [...] esildise põhjal toimunud hindamise tulemustest ja võimalike meetmete võtmise ajast.

7. Kui veebimajutusteenuse pakkuja leiab, et esildis ei sisalda selles kirjeldatud sisu hindamiseks piisavalt teavet, teatab ta sellest viivitamata pädevale asutusele või asjaomasele liidu asutusele ja täpsustab, millist täiendavat teavet või milliseid selgitusi oleks vaja.

Artikkel 6

Ennetavad meetmed

1. Veebimajutusteenuse pakkuja võtab [...] ***sõltuvalt terroristliku sisuga kokkupuutumise riskist ja ulatusest*** ennetavaid meetmeid, et kaitsta oma teenuseid terroristliku sisu levitamise eest. Need meetmed peavad olema tulemuslikud ja proportsionaalsed ning võtma arvesse terroristliku sisuga kokkupuutumise riski ja ulatust, kasutajate põhiõigusi ning sõna- ja teabevabaduse olulisust avatud ja demokraatlikus ühiskonnas.

2. Kui artikli 17 lõike 1 punktis c osutatud pädevat asutust on teavitatud vastavalt artikli 4 lõikele 9, palub ta veebimajutusteenuse pakkujal esitada kolme kuu jooksul pärast taotluse kättesaamist ja pärast seda vähemalt kord aastas aruande konkreetsete ennetavate meetmete kohta, mida ta on võtnud muu hulgas automaatsete vahendite abil, et:

   a) [...] ***tõkestada tõhusalt*** sellise sisu uuesti ***üleslaadimist***, [...] mis on varem eemaldatud või millele juurdepääs on blokeeritud, sest seda loetakse terroristlikuks sisuks;

   b) terroristlikku sisu avastada ja see kindlaks teha ning see kiiresti eemaldada või blokeerida juurdepääs sellele.

   Selline taotlus saadetakse veebimajutusteenuse pakkuja peamisesse tegevuskohta või teenusepakkuja määratud esindajale.

   Aruanded peavad sisaldama kogu asjakohast teavet, et artikli 17 lõike 1 punktis c osutatud pädev asutus saaks hinnata, kas ennetavad meetmed on tulemuslikud ja proportsionaalsed, ning anda muu hulgas oma hinnangu kasutatavate automaatsete vahendite toimimisele ja inimeste teostatava jälgimise ja kontrollimise mehhanismidele.

3. Kui artikli 17 lõike 1 punktis c osutatud pädev asutus leiab, et võetud ennetavad meetmed, millest on antud aru vastavalt lõikele 2, ei ole kokkupuutumise riski ja ulatuse leevendamiseks ja nendega toimetulemiseks piisavad, võib ta taotleda, et veebimajutusteenuse pakkuja võtaks konkreetseid täiendavaid ennetavaid meetmeid. Selle eesmärgi saavutamise nimel teeb veebimajutusteenuse pakkuja koostööd artikli 17 lõike 1 punktis c osutatud pädeva asutusega, et teha kindlaks konkreetsed meetmed, mille veebimajutusteenuse osutaja peab kehtestama, ning panna paika peamised eesmärgid ja kriteeriumid ja nende rakendamise ajakava.

4. Kui kolme kuu jooksul pärast lõikes 3 osutatud taotluse esitamist ei suudeta jõuda kokkuleppele, võib artikli 17 lõike 1 punktis c osutatud pädev asutus teha otsuse kehtestada konkreetsed täiendavad vajalikud ja proportsionaalsed ennetavad meetmed. Otsuses peab arvestama veebimajutusteenuse pakkuja majandusliku suutlikkusega ning selliste meetmete mõjuga kasutajate põhiõigustele ja sõna- ja teabevabaduse olulisusele. ***Kooskõlas käesoleva määruse eesmärgiga otsustab ennetavate meetmete laadi ja ulatuse üle artikli 17 lõike 1 punktis c osutatud pädev asutus.*** Selline otsus saadetakse veebimajutusteenuse pakkuja peamisesse tegevuskohta või teenusepakkuja määratud esindajale. Veebimajutusteenuse pakkuja annab artikli 17 lõike 1 punktis c osutatud pädeva asutuse kindlaksmääratud meetmete rakendamisest korrapäraselt aru.

5. Veebimajutusteenuse pakkuja võib igal ajal taotleda, et artikli 17 lõike 1 punktis c osutatud pädev asutus vaataks läbi ja vajaduse korral tühistaks vastavalt kas lõikes 2, 3 või 4 kirjeldatud taotluse või otsuse. Pädev asutus teeb põhjendatud otsuse mõistliku aja jooksul pärast seda, kui on saanud veebimajutusteenuse pakkuja taotluse.

Artikkel 7

Sisu ja seotud andmete säilitamine

1. Veebimajutusteenuse pakkuja säilitab vastavalt artiklitele 4, 5 ja 6 eemaldamiskorralduse või esildise põhjal või ennetavate meetmete tulemusena eemaldatud või blokeeritud terroristliku sisu ning terroristliku sisu eemaldamise tagajärjel eemaldatud seotud andmed, […] mis on vajalikud:

   a) halduslikus või kohtulikus korras toimuva kontrollimise jaoks,

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

2. Lõikes 1 osutatud terroristlikku sisu ja sellega seotud andmeid säilitatakse kuus kuud. Pädeva asutuse või kohtu taotluse korral säilitatakse terroristlikku sisu kauem, tingimusel et ja nii kaua kui see on vajalik lõike 1 punktis a osutatud poolelioleva halduslikus või kohtulikus korras toimuva kontrollimise jaoks.

3. Veebimajutusteenuse pakkuja tagab, et vastavalt lõigetele 1 ja 2 säilitatava terroristliku sisu ja sellega seotud andmete suhtes kohaldatakse asjakohaseid tehnilisi ja korralduslikke kaitsemeetmeid.

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

III JAGU
KAITSEMEETMED JA VASTUTUS

Artikkel 8

Läbipaistvuskohustused

1. Veebimajutusteenuse pakkuja esitab oma tingimustes terroristliku sisu levitamise vältimise põhimõtted, sealhulgas vajaduse korral sisulise selgituse ennetavate meetmete toimimise, kaasa arvatud automaatsete vahendite kasutamise kohta.

2. Veebimajutusteenuse pakkuja, [...] kellel on ***kokkupuude terroristliku sisuga***, avaldab igal aastal läbipaistvusaruande terroristliku sisu levitamise vastu võetud meetmete kohta.

3. Läbipaistvusaruanded peavad sisaldama vähemalt järgmist teavet:

   a) teave selle kohta, millised on veebimajutusteenuse pakkuja meetmed seoses terroristliku sisu avastamise, kindlakstegemise ja eemaldamisega;

   b) teave selle kohta, millised on veebimajutusteenuse pakkuja meetmed, et ***tõkestada tõhusalt*** [...] sellise sisu uuesti […] ***üleslaadimist***, mis on varem eemaldatud või millele juurdepääs on blokeeritud, sest seda loetakse terroristlikuks sisuks;

   c) nende terroristliku sisu ühikute arv, mis on eemaldatud või millele juurdepääs on blokeeritud vastavalt kas eemaldamiskorralduse, esildise või ennetavate meetmete kohaselt;

   d) ülevaade kaebuste esitamise menetlustest ja nende tagajärjed.

Artikkel 9

Kaitsemeetmed seoses ennetavate meetmete kasutamise ja rakendamisega

1. Kui veebimajutusteenuse pakkuja kasutab enda talletatava veebisisu puhul automaatseid vahendeid vastavalt käesolevale määrusele, peab ta pakkuma mõjusaid ja asjakohaseid kaitsemeetmeid tagamaks, et asjaomase sisu suhtes tehtud otsused, eelkõige terroristlikuks peetava sisu eemaldamise või sellele juurdepääsu blokeerimise otsused, on täpsed ja hästi põhjendatud.

2. Eeskätt peavad kaitsemeetmed hõlmama inimeste teostatavat jälgimist ja kontrolli siis, kui see on asjakohane, ja igal juhul siis, kui on tarvis üksikasjalikku hindamist, et teha kindlaks, kas tegemist on terroristliku sisuga.

Artikkel 10

Kaebuste lahendamise mehhanism

1. Veebimajutusteenuse pakkuja kehtestab mõjusad ja juurdepääsetavad mehhanismid, millele toetudes saab sisuteenuse pakkuja, kelle sisu on eemaldatud või kelle sisule juurdepääs on blokeeritud artikli 5 kohase esildise või artikli 6 kohaste ennetavate meetmete tõttu, esitada kaebuse veebimajutusteenuse pakkuja tegevuse kohta ja nõuda sisu taastamist.

2. Veebimajutusteenuse pakkuja vaatab kõik saadud kaebused kiiresti läbi ja kui sisu eemaldamine või juurdepääsu blokeerimine sellele oli alusetu, taastab sisu ilma põhjendamatu viivituseta. Ta teavitab kaebuse esitajat läbivaatamise tulemustest.

Artikkel 11

Sisuteenuse pakkujale esitatav teave

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

2. Sisuteenuse pakkuja taotluse korral teavitab veebimajutusteenuse pakkuja sisuteenuse pakkujat sisu eemaldamise või sellele juurdepääsu blokeerimise põhjustest ja otsuse vaidlustamise võimalustest.

3. Lõigete 1 ja 2 kohast kohustust ei kohaldata, kui pädev asutus otsustab, et avalikustamisest tuleb loobuda 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. ***Seda ajavahemikku võib pikendada ühekordselt veel kuue nädala võrra, kui see on õigustatud.*** Sellisel juhul ei avalikusta veebimajutusteenuse pakkuja terroristliku sisu eemaldamise või sellele juurdepääsu tõkestamise kohta mitte mingisugust teavet.

IV JAGU

Pädevate asutuste, liidu asutuste ja veebimajutusteenuse pakkujate koostöö

Artikkel 12

Pädevate asutuste võimekus

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

Artikkel 13

Veebimajutusteenuse pakkujate, pädevate asutuste ja vajaduse korral [...] ***pädevate*** *liidu asutuste koostöö*

1. Liikmesriikide pädevad asutused jagavad eemaldamiskorralduste ja esildiste küsimustes teavet, koordineerivad ja teevad koostööd omavahel ning vajaduse korral [...] ***pädevate*** liidu asutustega (näiteks Europoliga), et vältida topelttööd, parandada koordineerimist ja vältida sekkumist teistes liikmesriikides toimuvatesse uurimistesse.

2. Artikli 6 kohaselt võetud meetmete ja artikli 18 kohaste täitemeetmete puhul jagavad liikmesriikide pädevad asutused teavet, koordineerivad ja teevad koostööd artikli 17 lõike 1 punktides c ja d osutatud pädeva asutusega. Liikmesriigid tagavad, et artikli 17 lõike 1 punktides c ja d osutatud pädeva asutuse käsutuses on kogu asjakohane teave. Seda eesmärki silmas pidades näevad liikmesriigid ette asjakohased sidekanalid või -mehhanismid, et tagada asjaomase teabe õigeaegne jagamine.

3. ***Käesoleva määruse tõhusaks rakendamiseks ja dubleerimise vältimiseks*** võivad liikmesriigid ja veebimajutusteenuse pakkujad otsustada kasutada spetsiaalseid vahendeid, sealhulgas [...] vajaduse korral [...] ***pädevate*** liidu asutuste, näiteks Europoli loodud vahendeid, et aidata kaasa eeskätt järgmisele tegevusele:

a) artikli 4 kohaste eemaldamiskorralduste töötlemine ja nende kohta käiv tagasiside;

b) artikli 5 kohaste esildiste töötlemine ja nende kohta käiv tagasiside;

c) koostöö, et teha kindlaks ja rakendada artikli 6 kohased ennetavad meetmed.

4. Kui veebimajutusteenuse pakkuja saab teadlikuks mis tahes tõendusmaterjalist terroriakti kohta, teavitab ta sellest viivitamata asjaomases liikmesriigis või asjaomastes liikmesriikides kuritegude uurimise ja nende eest süüdistuse esitamisega tegelevaid pädevaid asutusi. ***Kui asjaomast liikmesriiki või asjaomaseid liikmesriike ei ole võimalik tuvastada, [...] teavitavad*** veebimajutusteenuse pakkujad […] ***artikli 14 lõike 3 kohast kontaktpunkti liikmesriigis, kus on nende peamine tegevuskoht või esindaja ning*** edastavad selle teabe ka Europolile asjakohaste järelmeetmete võtmiseks.

Artikkel 14

Kontaktpunktid

1. Veebimajutusteenuse pakkuja loob kontaktpunkti, mille kaudu võtta elektrooniliselt vastu eemaldamiskorraldusi ja esildisi ning tagada nende kiire töötlemine vastavalt artiklitele 4 ja 5. Ta tagab, et teave selle kohta on avalikult kättesaadav.

2. Lõikes 1 osutatud teabes tuleb ära märkida määruses 1/58 nimetatud liidu ametlikud keeled, milles võib kontaktpunkti poole pöörduda ja mida kasutatakse edasiseks suhtlemiseks artiklite 4 ja 5 kohaste eemaldamiskorralduste ja esildiste puhul. Nende keelte hulka peab kuuluma vähemalt üks selle liikmesriigi ametlik keel, kus asub veebimajutusteenuse pakkuja peamine tegevuskoht või kus elab või tegutseb tema artiklis 16 osutatud esindaja.

3. Liikmesriigid loovad kontaktpunkti, kes tegeleb nende tehtud eemaldamiskorralduse ja esildiste kohta esitatud selgitamisnõuete ja tagasisidega. Teave kontaktpunkti kohta tehakse avalikult kättesaadavaks.

V JAGU
RAKENDAMINE JA TÄITMISE TAGAMINE

Artikkel 15

Jurisdiktsioon

1. Artiklite 6, 18 ja 21 kohaldamisel kuulub jurisdiktsioon liikmesriigile, kus on veebimajutusteenuse pakkuja peamine tegevuskoht. Kui veebimajutusteenuse pakkuja peamine tegevuskoht ei ole üheski liikmesriigis, loetakse ta selle liikmesriigi jurisdiktsiooni alla kuuluvaks, kus elab või tegutseb tema artiklis 16 osutatud esindaja. ***Artiklite 4 ja 5 kohaldamisel on jurisdiktsioon igal liikmesriigil, sõltumata sellest, kus on veebimajutusteenuse pakkuja peamine tegevuskoht või kus asub tema määratud esindaja.***

2. Kui veebimajutusteenuse pakkuja ei suuda esindajat määrata, kuulub jurisdiktsioon kõigile liikmesriikidele. ***Kui liikmesriik otsustab oma jurisdiktsiooni kasutada, teavitab ta kõiki teisi liikmesriike.***

[…] […]

Artikkel 16

Esindaja

1. Veebimajutusteenuse pakkuja, kellel ei ole liidus tegevuskohta, kuid kes pakub liidus teenuseid, määrab kirjalikult oma esindajaks liidus füüsilise või juriidilise isiku, et see tegeleks pädevate asutuste käesoleva määruse põhjal tehtud eemaldamiskorralduste, esildiste, taotluste ja otsuste kättesaamise, järgimise ja täitmise tagamisega. Esindaja elab või tegutseb ühes liikmesriikidest, kus veebimajutusteenuse pakkuja teenuseid pakub.

2. Veebimajutusteenuse pakkuja usaldab esindajale lõikes 1 osutatud eemaldamiskorralduste, esildiste, taotluste ja otsuste kättesaamise, järgimise ja nende täitmise tagamise asjaomase veebimajutusteenuse pakkuja nimel. Veebimajutusteenuse pakkuja annab oma esindajale vajalikud õigused ja vahendid, et teha pädevate asutustega koostööd ja järgida kõnealuseid otsuseid ja korraldusi.

3. Käesolevast määrusest tulenevate kohustuste täitmata jätmise korral võib määratud esindaja vastutusele võtta, ilma et see piiraks vastutust või kohtumenetlusi, mis võidakse algatada veebimajutusteenuse pakkuja suhtes.

4. Veebimajutusteenuse pakkuja teatab määramisest esindaja elu- või tegutsemiskoha liikmesriigi artikli 17 lõike 1 punktis d osutatud pädevale asutusele. Teave esindaja kohta tehakse avalikult kättesaadavaks.

VI JAGU
LÕPPSÄTTED

Artikkel 17

Pädevate asutuste määramine

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

   a) artikli 4 kohaste eemaldamiskorralduste tegemine;

   b) terroristliku sisu avastamine, kindlakstegemine ja sellekohase esildise tegemine veebimajutusteenuse pakkujale vastavalt artiklile 5;

   c) ennetavate meetmete rakendamise jälgimine vastavat artiklile 6;

   d) käesolevast määrusest tulenevate kohustuste täitmise tagamine karistuste abil vastavalt artiklile 18.

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

Artikkel 18

Karistused

1. Liikmesriigid näevad ette õigusnormid karistuste kohta, mida kohaldatakse, kui veebimajutusteenuse pakkuja rikub käesolevast määrusest tulenevaid kohustusi, ning võtavad kõik vajalikud meetmed, et tagada nende karistuste rakendamine. Karistusi kohaldatakse selliste kohustuste rikkumise puhul, mis on ette nähtud:

   a) artikli 3 lõikega 2 (veebimajutusteenuse pakkuja tingimused);

   b) artikli 4 lõigetega 2 ja 6 (eemaldamiskorralduste rakendamine ja tagasiside nende kohta);

c) artikli 5 lõigetega 5 ja 6 (esildiste hindamine ja tagasiside nende kohta);

d) artikli 6 lõigetega 2 ja 4 (aruanded ennetavate meetmete kohta ja meetmete vastuvõtmine pärast seda, kui on tehtud otsus konkreetsete ennetavate meetmete kehtestamiseks);

e) artikliga 7 (andmete säilitamine);

f) artikliga 8 (läbipaistvus);

g) artikliga 9 (ennetavate meetmetega seotud kaitsemeetmed);

h) artikliga 10 (kaebuste lahendamise menetlused);

i) artikliga 11 (sisuteenuse pakkujale esitatav teave);

j) artikli 13 lõikega 4 (teave terroriakte käsitleva tõendusmaterjali kohta);

k) artikli 14 lõikega 1 (kontaktpunktid);

l) artikliga 16 (esindaja määramine).

2. Kehtestatud karistused peavad olema tõhusad, proportsionaalsed ja hoiatavad. Liikmesriigid teatavad kõnealustest õigusnormidest ja meetmetest komisjonile hiljemalt [... *kuu jooksul pärast käesoleva määruse jõustumist*], samuti teatavad nad viivitamata kõigist neid mõjutavatest hilisematest muudatustest.

3. Liikmesriigid tagavad, et karistuste liigi ja taseme kindlaksmääramisel võtavad pädevad asutused arvesse kõiki asjaomaseid asjaolusid, muu hulgas järgmist:

a) rikkumise laad, raskus ja kestus;

b) kas rikkumine pandi toime tahtlikult või hooletusest;

c) vastutava juriidilise ***või füüsilise*** isiku varasemad rikkumised;

d) vastutava juriidilise ***või füüsilise*** isiku rahaline usaldusväärsus;

e) veebimajutusteenuse pakkuja valmidus teha pädevate asutustega koostööd.

4. Liikmesriigid tagavad, et artikli 4 lõikest 2 tulenevate kohustuste süstemaatilise eiramise korral rakendatakse rahalist karistust, mille summa on kuni 4 % veebimajutusteenuse pakkuja eelmise majandusaasta kogukäibest.

Artikkel 19

Eemaldamiskorralduse vormide tehnilised nõuded ja muudatused

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

2. Komisjonil on õigus võtta I, II ja III lisa muutmiseks vastu selliseid delegeeritud õigusakte, et leida reaalne lahendus võimalikule vajadusele teha parandusi eemaldamiskorralduse vormide sisus ja selliste vormide sisus, millega antakse teada, et eemaldamiskorraldust ei ole võimalik täita.

Artikkel 20

Delegeeritud volituste rakendamine

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

2. Komisjonile antakse alates [*käesoleva määruse kohaldamise alguskuupäev*] määramata ajaks õigus võtta vastu artiklis 19 osutatud delegeeritud õigusakte.

3. Euroopa Parlament või nõukogu võib 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 vastuväiteid või kui Euroopa Parlament ja nõukogu on enne selle tähtaja möödumist komisjonile teatanud, et nad ei esita vastuväiteid. Euroopa Parlamendi või nõukogu algatusel pikendatakse seda tähtaega kahe kuu võrra.

Artikkel 21

Jälgimine

1. Liikmesriigid koguvad oma pädevatelt asutustelt ja oma jurisdiktsiooni alla kuuluvatelt veebimajutusteenuse pakkujatelt teavet meetmete kohta, mida need on võtnud vastavalt käesolevale määrusele, ning saadavad selle teabe komisjonile iga aasta [31. märtsiks]. Kõnealune teave hõlmab järgmist:

   a) teave tehtud eemaldamiskorralduste ja esildiste arvu kohta ning nende terroristliku sisu ühikute arv, mis on eemaldatud või millele juurdepääs on blokeeritud, kaasa arvatud asjaomased ajakavad vastavalt artiklitele 4 ja 5;

b) teave konkreetsete ennetavate meetmete kohta, mis on võetud vastavalt artiklile 6, kaasa arvatud nende terroristliku sisu ühikute arv, mis on eemaldatud või millele juurdepääs on blokeeritud ja asjaomased ajakavad;

c) teave selle kohta, mitu kaebuste lahendamise menetlust on algatatud ja kui palju meetmeid on veebimajutusteenuse pakkujad võtnud vastavalt artiklile 10;

d) teave selle kohta, mitu õiguskaitsemenetlust on algatatud ja millised otsused on pädev asutus siseriikliku õiguse alusel teinud.

2. Komisjon koostab hiljemalt [*üks aasta pärast käesoleva määruse kohaldamise alguskuupäeva*] käesoleva määruse väljundite, tulemuste ja mõju jälgimiseks üksikasjaliku kava. Jälgimiskavas 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 jälgida 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. Komisjoni aruandes võetakse arvesse teavet artikli 21 kohase jälgimise kohta ja artikli 8 kohastest läbipaistvuskohustustest tulenevat teavet. Liikmesriigid esitavad komisjonile teabe, mida on vaja aruande koostamiseks.

Artikkel 23

Hindamine

Komisjon hindab käesolevat määrust mitte varem kui [*kolm aastat pärast käesoleva määruse kohaldamise alguskuupäeva*] ning esitab Euroopa Parlamendile ja nõukogule aruande selle kohaldamise kohta, kaasa arvatud kaitsemehhanismide mõjususe toimimise kohta. Vajaduse korral esitatakse koos aruandega seadusandlikud ettepanekud. Liikmesriigid esitavad komisjonile teabe, mida on vaja aruande koostamiseks.

Artikkel 24

Jõustumine

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

Seda kohaldatakse alates [***12*** kuud pärast jõustumist].

Käesolev määrus on tervikuna siduv ja vahetult kohaldatav kõikides liikmesriikides.

Brüssel,

Euroopa Parlamendi nimel *president*	*Nõukogu nimel* *eesistuja*