EUROOPA
KOMISJON

Brüssel, 12.9.2018
COM(2018) 640 final

2018/0331 (COD)

Ettepanek:

EUROOPA PARLAMENDI JA NÕUKOGU MÄÄRUS

terroristliku veebisisu levitamise tõkestamise kohta

Euroopa Komisjoni panus juhtide kohtumisse,
mis toimub Salzburgis 19.–20. septembril 2018

{SEC(2018) 397 final} - {SWD(2018) 408 final} - {SWD(2018) 409 final}

SELETUSKIRI

1. ETTEPANEKU TAUST

1.1. Ettepaneku põhjused ja eesmärgid

Et internet on kõikjal, on selle kasutajatel võimalus suhelda, koostööd teha, aega veeta ning teavet ja sisu luua, saada ja vahetada sadade miljonite inimestega kõikjal maailmas. Veebiplatvormid suurendavad oluliselt kasutajate majanduslikku ja sotsiaalset heaolu kogu liidus ja mujal. Ent võimalus jõuda minimaalsete kuludega nii suure auditooriumini paelub ka kurjategijaid, kelle soov on internetti ebaseaduslikel eesmärkidel kuritahtlikult kasutada. Hiljutised ELi territooriumil toime pandud terrorirünnakud on näidanud, et terroristid kasutavad internetti kuritahtlikult eesmärgiga õpetada välja ja värvata toetajaid, valmistada ette ja hõlbustada terroritegevust, ülistada toimepandud hirmutegusid, kutsuda teisi oma eeskuju järgima ning süstida üldsusse hirmu.

Sel eesmärgil veebis jagatavat terroristlikku sisu levitatakse veebimajutusteenuse pakkujate kaudu, kes lubavad üles laadida kolmandate isikute sisu. Mitme hiljutise Euroopas toimunud terrorirünnaku puhul on tõendatud, et ebaseaduslik veebisisu on kaasa aidanud niinimetatud üksikute huntide radikaliseerumisele ja ajendanud neid rünnakuid toime panema. Lisaks sellele, et ebaseaduslikul veebisisul on märkimisväärne negatiivne mõju üksikisikutele ja kogu ühiskonnale, kahandab see ka kasutajate usaldust interneti vastu ning kahjustab mõjutatud ettevõtete ärimudeleid ja mainet. Lisaks suurtele sotsiaalmeediaplatvormidele kasutavad terroristid kuritahtlikult üha rohkem ära ka väiksemaid teenusepakkujaid, kes osutavad üleilmselt erinevaid veebimajutusteenuseid. Interneti kuritahtlik kasutamine tõstab esile seda, et veebiplatvormidel on eriline ühiskondlik vastutus kaitsta oma kasutajaid kokkupuute eest terroristliku sisuga ja et selline sisu kujutab enesest tõsist ohtu kogu ühiskonna turvalisusele.

Vastusena ametivõimude üleskutsetele on veebimajutusteenuse pakkujad võtnud teatavad meetmed, et võidelda nende teenuste kaudu levitatava terroristiliku sisuga. Vabatahtlike raamistike ja partnerluste, sealhulgas 2015. aasta detsembris Euroopa julgeoleku tegevuskava raames käivitatud ELi internetifoorumi varal on tehtud edusamme. ELi internetifoorum on soodustanud liikmesriikide ja veebimajutusteenuse pakkujate vabatahtlikku koostööd ja selliste meetmete võtmist, millega piiratakse terroristliku veebisisu kättesaadavust ja võimestatakse kodanikuühiskonda levitama internetis laialdasemalt mõjusaid alternatiivseid seisukohti. Need jõupingutused on aidanud tihendada koostööd, pannes ettevõtted riigi ametiasutuste ja samuti Europoli internetisisust teavitamise üksuse esildistele paremini reageerima, võtta vabatahtlikke ennetavaid meetmeid, mille eesmärk on parandada terroristliku sisu automaatset avastamist, tihendada koostööd valdkonna ettevõtetega, sealhulgas töötada välja räsiandmebaas, millega välditakse teadaoleva terroristliku sisu üleslaadimist baasiga ühendatud platvormidel, samuti suurendada jõupingutuste läbipaistvust. Ehkki koostöö ELi internetifoorumi raames peaks jätkuma ka tulevikus, on samuti selgeks saanud, et vabatahtlikest kokkulepetest aitab ainult teatud piirini. Esiteks ei osale kõik mõjutatud veebimajutusteenuse pakkujad foorumi tegevuses ja teiseks ei ole veebimajutusteenuse pakkujate edusammud tervikuna olnud küllalt ulatuslikud ja kiired selleks, et kõnealust probleemi asjakohaselt käsitleda.

Seda piiratust arvestades on ilmne, et Euroopa Liidul tuleb võtta tõhustatud meetmeid terroristliku veebisisu vastu. 1. märtsil 2018 võttis komisjon vastu soovituse meetmete kohta,

millega tulemuslikult võidelda ebaseadusliku veebisisu vastu, tuginedes komisjoni septembrikuisele teatisele,[1] samuti ELi internetifoorumi raames tehtud jõupingutustele. Soovituse eraldi peatükis oli ära toodud mitu meedet terroristliku propaganda üleslaadimise ja jagamise tulemuslikuks tõkestamiseks, nagu esildise tegemise protsessi täiustamine, esildisele vastamine ühe tunni jooksul, tõhusam ennetav avastamine, sisu tulemuslik eemaldamine ja küllaldased kaitsemeetmed terroristliku sisu õigeks hindamiseks[2].

Vajadusest tõhustada terroristliku veebisisu vastaseid meetmeid on teada andnud ka ELi liikmesriikide üleskutsed; mõned liikmesriigid on juba võtnud vastu õigusakte või andnud teada kavatsusest seda teha. Pärast terrorirünnakute lainet ELis ja võttes arvesse asjaolu, et terroristlik veebisisu on endiselt hõlpsalt kättesaadav, kutsus Euroopa Ülemkogu oma 22. ja 23. juunil 2017 toimunud kohtumisel sektoris tegutsejaid „töötama välja uusi tehnoloogiaid ja vahendeid, et parandada terroriaktide toimepanemist õhutava veebisisu automaatset tuvastamist ja kõrvaldamist. Seda tuleks vajaduse korral täiendada asjakohaste seadusandlike meetmetega ELi tasandil.“ 28. juunil 2018 tervitas Euroopa Ülemkogu „komisjoni kavatsust esitada seadusandlik ettepanek, mille eesmärk on parandada vihkamist ja terroriaktide toimepanemist õhutava sisu kindlakstegemist ja eemaldamist“. Lisaks sellele kutsus Euroopa Parlament oma 15. juuni 2017. aasta resolutsioonis veebiplatvormide ja digitaalse ühtse turu kohta asjaomaseid platvorme üles „tugevdama meetmeid ebaseadusliku ja kahjuliku infosisu tõkestamiseks“ ning palus komisjonil esitada ettepanekud nende küsimuste lahendamiseks.

Nende probleemide lahendamiseks ning vastusena liikmesriikide ja Euroopa Parlamendi üleskutsetele on komisjon esitanud käesoleva ettepaneku, mille eesmärk on luua selge ja ühtne õigusraamistik, et tõkestada veebimajutusteenuste kuritahtlikku kasutamist terroristliku veebisisu levitamiseks eesmärgiga tagada digitaalse ühtse turu sujuv toimimine ning säilitada samal ajal usaldus ja turvalisus. Käesoleva määruse eesmärk on luua selgus seoses veebimajutusteenuse pakkujate kohustusega võtta kõik asjakohased, mõistlikud ja proportsionaalsed meetmed, mis on vajalikud selleks, et tagada nende teenuste ohutus ning terroristlik veebisisu kiiresti ja tulemuslikult avastada ja eemaldada, võttes arvesse sõna- ja teabevabaduse olulisust avatud ja demokraatlikus ühiskonnas. Samuti kehtestatakse sellega mitu vajalikku kaitsemeedet, mis on ette nähtud selliste põhiõiguste tagamiseks nagu sõna- ja teabevabadus demokraatlikus ühiskonnas, ja antakse võimalus pöörduda kohtusse, mis on tagatud ELi lepingu artiklis 19 ja Euroopa Liidu põhiõiguste harta artiklis 47 sätestatud õigusega tõhusale õiguskaitsevahendile.

Ettepanekuga kehtestatakse minimaalsed hoolsuskohustused veebimajutusteenuse pakkujatele, sealhulgas mõned erieeskirjad ja -kohustused, samuti kohustused liikmesriikidele, püüdes nii suurendada praegu terroristliku veebisisu avastamiseks, kindlakstegemiseks ja kõrvaldamiseks kasutatavate meetmete tulemuslikkust, rikkumata seejuures põhiõigusi, nagu sõna- ja teabevabadus. Selline ühtne õigusraamistik hõlbustab internetipõhiste teenuste pakkumist kogu digitaalsel ühtsel turul, tagab võrdsed võimalused kõigi selliste veebimajutusteenuste pakkujate jaoks, kelle teenused on suunatud Euroopa Liidule, ning loob kindla õigusraamistiku terroristliku sisu avastamiseks ja eemaldamiseks koos kohaste kaitsemeetmetega põhiõiguste kaitseks. Eriti just läbipaistvusnõuded suurendavad kodanike ja eriti internetikasutajate usaldust ning parandavad ettevõtete vastutust ja nende tegevuse läbipaistvust, sealhulgas ametiasutuste vaatevinklist. Samuti kehtestatakse ettepanekuga kohustus näha ette õiguskaitse- ja kaebuste esitamise mehhanismid, et tagada

[1] Teatis (COM(2017) 555 final), mis käsitleb võitlust ebaseadusliku veebisisuga.

[2] 1. märtsi 2018. aasta soovitus (C(2018)1177 final) meetmete kohta, millega tulemuslikult võidelda ebaseadusliku veebisisu vastu.

kasutajatele võimalus oma sisu eemaldamine vaidlustada. Liikmesriikidele kehtivad kohustused aitavad nende eesmärkide saavutamisele kaasa, samuti parandavad asjaomaste asutuste suutlikkust võtta asjakohaseid meetmeid terroristliku veebisisu vastu ja võidelda kuritegevusega. Kui veebimajutusteenuse pakkujad käesoleva määruse nõudeid ei täida, on liikmesriikidel õigus määrata karistusi.

1.2. Kooskõla poliitikavaldkonnas praegu kehtiva ELi õigusraamistikuga

Käesolev ettepanek on kooskõlas digitaalset ühtset turgu käsitleva liidu õigustikuga, eriti e-kaubanduse direktiiviga. Ennekõike ei tohiks mitte ükski meede (sealhulgas ennetusmeede), mille veebimajutusteenuse pakkuja võtab kooskõlas käesoleva määrusega, tingida seda, et kõnealune teenusepakkuja ei saa kasutada vastutusest vabastamise erandit, mis on teatavatel tingimustel ette nähtud e-kaubanduse direktiivi artikliga 14. Põhimõtteliselt ei tohiks riigi ametiasutuse otsus võtta proportsionaalseid ja ennetavaid meetmeid viia selleni, et liikmesriikidele kehtestatakse direktiivi 2000/31/EÜ artikli 15 lõikes 1 määratletud üldine jälgimiskohustus. Võttes aga arvesse terroristiliku sisu levitamisega seonduvat eriti suurt ohtu, võidakse käesoleva määruse kohaselt tehtud otsustes sellest põhimõttest ELi raamistikus erandkorras kõrvale kalduda. Enne sellise otsuse vastuvõtmist peaks pädev asutus leidma õiglase tasakaalu avaliku julgeoleku vajaduste ning riivatud huvide ja põhiõiguste vahel, eriti seoses sõna- ja teabevabaduse ja ettevõtlusvabadusega ning isikuandmete ja eraelu puutumatuse kaitsega. Seda e-kaubanduse direktiivis väljendatud tasakaalu tuleks kajastada ja arvesse võtta veebimajutusteenuse pakkujate hoolsuskohustuste juures.

Samuti on ettepanek sidus ja tihedalt kooskõlas direktiiviga (EL) 2017/541 terrorismivastase võitluse kohta, mille eesmärk on ühtlustada terroriakte kriminaliseerivad liikmesriikide õigusaktid. Terrorismivastase võitluse direktiivi artikliga 21 pannakse liikmesriikidele kohustus võtta meetmed, millega tagatakse terroriakti toimepanemisele kutsumisega piirduva veebisisu eemaldamine ja jäetakse võetavate meetmete valik liikmesriikide hoolde. Käesoleva määruse ennetavat iseloomu arvestades hõlmab see mitte ainult terrorismile õhutavat materjali, vaid ka värbamiseks või väljaõppeks mõeldud materjali, kajastades muid terroristliku tegevusega seotud kuritegusid, mida direktiiv (EL) 2017/541 samuti hõlmab. Eesmärgiga vähendada terroristliku veebisisu kättesaadavust kehtestatakse käesoleva määrusega veebimajutusteenuse pakkujale otseselt hoolsuskohustus, mille kohaselt terroristlik sisu tuleb eemaldada, ja ühtlustatakse eemaldamiskorraldustega seotud menetlusi.

Määrus täiendab tulevases audiovisuaalmeedia teenuste direktiivis sätestatud eeskirju, kuna selle isikuline ja materiaalne kohaldamisala on laiem. Määrus hõlmab mitte ainult videojagamisplatvorme, vaid kõiki erinevaid veebimajutusteenuse pakkujaid. Lisaks hõlmab see peale videote ka kujutisi ja teksti. Peale selle läheb käesolev määrus direktiivist kaugemale sisuliste sätete vallas, kuna sellega ühtlustatakse terroristliku sisu eemaldamise ja ennetavate meetmete suhtes kehtivaid norme.

Määruse ettepanek tugineb komisjoni 2018. aasta märtsikuisele soovitusele[3] ebaseadusliku sisu kohta. Soovitus on endiselt jõus ja kõik need, kellel on oma osa ebaseadusliku sisu, sealhulgas terroristliku sisu kättesaadavuse piiramises, peaksid oma jõupingutustes püsima soovituses esitatud meetmete kursil.

[3] 1. märtsi 2018. aasta soovitus (C(2018)1177 final) meetmete kohta, millega tulemuslikult võidelda ebaseadusliku veebisisu vastu.

1.3. Kavandatava määruse kokkuvõte

Ettepaneku isikuline kohaldamisala hõlmab veebimajutusteenuse pakkujaid, kes pakuvad oma teenuseid liidus, sõltumata nende asukohast või suurusest. Kavandatava õigusaktiga kehtestatakse mitu meedet, et tõkestada veebimajutusteenuste kuritahtlikku kasutamist terroristliku veebisisu levitamiseks, tagamaks digitaalse ühtse turu sujuv toimimine ning säilitada samal ajal usaldus ja turvalisus. Ebaseadusliku terroristliku sisu määratlus on kooskõlas direktiivis (EL) 2017/541 esitatud terroriakti määratlusega ja on määratletud kui teave, mida kasutatakse terroriaktide sooritamisele õhutamiseks ja selle ülistamiseks, kutsudes üles terroriaktide sooritamisele kaasa aitama ja andes selleks juhiseid, ning mis propageerib terroristlikes rühmitustes osalemist.

Selleks et tagada terroristliku veebisisu eemaldamine, nähakse määrusega ette eemaldamiskorraldus, mille liikmesriigi pädev asutus võib teha haldus- või kohtuotsuse vormis. Sellistel juhtudel on veebimajutusteenuse pakkuja kohustatud ühe tunni jooksul sisu eemaldama või sellele juurdepääsu blokeerima. Lisaks ühtlustatakse määrusega miinimumnõuded esildistele, mille liikmesriikide pädevad asutused ja liidu asutused, nagu Europol, teevad veebimajutusteenuse pakkujatele, et nad hindaksid neid lähtuvalt oma tingimustest. Samuti nähakse määrusega ette, et veebimajutusteenuse pakkujad peavad vajaduse korral võtma ennetavad meetmed, mis vastavad riski tasemele, ja terroristliku sisu oma teenustest eemaldama, muu hulgas võttes kasutusele vahendid selle automaatseks avastamiseks.

Koos terroristliku veebisisu vähendamiseks kavandatud meetmetega võetakse mitu keskse tähtsusega kaitsemeedet, et tagada põhiõiguste täielik kaitse. Osana meetmetest, mille eesmärk on kaitsta eksliku eemaldamise eest sisu, mis ei ole terroristlik, kehtestatakse ettepanekuga kohustus näha ette õiguskaitse- ja kaebuste esitamise mehhanismid, et tagada kasutajatele võimalus oma sisu eemaldamine vaidlustada. Lisaks sellele kehtestatakse määrusega läbipaistvusnõuded veebimajutusteenuse pakkujate poolt terroristliku sisu suhtes võetud meetmetele, tagades seeläbi vastutuse kasutajate, kodanike ja ametiasutuste ees.

Samuti pannakse määrusega liikmesriikidele kohustus tagada, et nende pädevatel asutustel on vajalik suutlikkus terroristliku veebisisu korral sekkumiseks. Lisaks sellele on liikmesriikidel kohustus üksteist teavitada ja omavahel koostööd teha ning nad võivad kasutada Europoli loodud kanaleid, et tagada eemaldamiskorralduste ja esildiste koordineeritus. Samuti nähakse määrusega ette, et veebimajutusteenuse pakkujad peavad andma üksikasjalikumalt aru võetud meetmetest ja teavitama õiguskaitseasutusi, kui nad avastavad sisu, mis kujutab enesest ohtu elule või turvalisusele. Lisaks on veebimajutusteenuse pakkujatel kohustus säilitada eemaldatud sisu: see toimib kaitsena eksliku eemaldamise eest ja tagab, et võimalikud terroriaktide tõkestamisel, avastamisel, uurimisel ja nende eest vastutusele võtmisel kasutatavad tõendid ei lähe kaotsi.

2. ÕIGUSLIK ALUS, SUBSIDIAARSUS JA PROPORTSIONAALSUS

2.1. Õiguslik alus

Õiguslik alus on Euroopa Liidu toimimise lepingu artikkel 114, mis võimaldab kehtestada meetmeid, mille eesmärk on tagada siseturu toimimine.

Artikkel 114 on kohane õiguslik alus selleks, et ühtlustada tingimused, mille alusel veebimajutusteenuse pakkujad pakuvad digitaalsel ühtsel turul piiriüleselt teenuseid, ja käsitleda liikmesriikide sätete erinevusi, mis võivad vastasel juhul takistada siseturu toimimist. Samuti ennetab see tulevaste majandustegevust tõkestavate tegurite esilekerkimist tulenevalt siseriiklike õigusnormide võimalikust erinevast arengust.

Ka saab ELi toimimise lepingu artiklit 114 kasutada kohustuste kehtestamiseks teenuseosutajatele asukohaga väljaspool ELi territooriumi, kui nende teenuste osutamine mõjutab siseturgu, kuna see on vajalik siseturuga seotud soovitud eesmärgi saavutamiseks.

2.2. Vahendi valik

Euroopa Liidu toimimise lepingu artikliga 114 antakse liidu seadusandjale võimalus võtta vastu määrusi ja direktiive.

Kuna ettepanek puudutab selliste teenuseosutajate teenuseid, kes pakuvad oma teenuseid tavaliselt rohkem kui ühes liikmesriigis, takistaks nende normide erinev kohaldamine mitmes liikmesriigis tegutsevatel teenuseosutajatel teenuseid osutada. Määrus võimaldab kehtestada ühe ja sama kohustuse ühtemoodi kogu liidus, on otsekohaldatav, tagab selguse ja suurema õiguskindluse ning hoiab ära lahknevused normide ülevõtmisel siseriiklikku õigusesse. Nimetatud põhjustel on määrus kõige asjakohasem vahend.

2.3. Subsidiaarsus

Käsitletavate probleemide piiriülest mõõdet arvesse võttes tuleb ettepanekus esitatud meetmed eesmärkide saavutamiseks võtta vastu liidu tasandil. Internet on oma olemuselt piiriülene ja ühes liikmesriigis asuva teenuseosutaja majutatavale sisule pääseb tavaliselt juurde kõigist teistest liikmesriikidest.

Siseriiklikud terroristliku veebisisuga võitlemise õigusnormid on ilmselgelt killustunud ja ohud üha kasvavad. See paneb ettevõtjatele erinevate eeskirjade täitmise koorma, loob neile ebavõrdsed tingimused ja põhjustab turvalünki.

Seega suurendavad ELi tasandi meetmed õiguskindlust ja veebimajutusteenuse pakkujate poolt terroristliku veebisisu vastu võetud meetmete tulemuslikkust. Need peaksid võimaldama rohkematel ettevõtetel (sealhulgas sellistel ettevõtetel, kelle asukoht on väljaspool Euroopa Liitu) meetmeid võtta, kindlustades nii digitaalse ühtse turu terviklust.

See õigustab vajadust ELi meetmete järele, nagu see kajastus Euroopa Ülemkogu 2018. aasta juuni järeldustes, millega kutsuti komisjoni üles esitama kõnealuses valdkonnas seadusandlik ettepanek.

2.4. Proportsionaalsus

Ettepanekuga kehtestatakse veebimajutusteenuse pakkujate suhtes normid, mille kohaselt nad peavad võtma meetmeid terroristliku sisu kiireks eemaldamiseks oma teenustest. Ettepaneku peamised elemendid piirduvad poliitikaeesmärkide saavutamiseks vajalikuga.

Ettepanekus arvestatakse veebimajutusteenuse pakkujate koormuse ja kaitsemeetmetega, sealhulgas sõna- ja teabevabaduse ning samuti muude põhiõiguste kaitsega. Ühe tunni pikkune eemaldamistähtaeg kehtib ainult eemaldamiskorralduste suhtes, kuna nende puhul on pädevad asutused kohtulikule kontrollile alluva otsusega tuvastanud ebaseaduslikkuse. Esildiste puhul kehtib nõue kehtestada meetmed, mis hõlbustavad terroristliku sisu kiiret hindamist, kehtestamata siiski selle eemaldamise kohustust või maksimaalseid tähtaegu. Lõplik otsus on vabatahtlik ja selle teeb veebimajutusteenuse pakkuja. Ettevõtete koormust sisu hindamisel kergendab asjaolu, et liikmesriikide pädevad asutused ja liidu asutused annavad selgitusi selle kohta, miks sisu võidakse pidada terroristlikuks sisuks. Vajaduse korral võtavad veebimajutusteenuse pakkujad ennetavaid meetmeid eesmärgiga kaitsta oma teenuseid terroristliku sisu levitamise eest. Ennetavaid meetmeid puudutavad erinõuded kehtivad ainult nende veebimajutusteenuse pakkujate suhtes, kellel on terroristliku sisuga kokkupuude, millest annab tunnistust lõplikuks muutunud eemaldamiskorralduse saamine, ning need peaksid vastama riski tasemele ja ettevõtte ressurssidele. Eemaldatud sisu ja sellega

seotud andmete säilitamine on piiratud ajavahemikuga, mis on haldus- või kohtuliku kontrolli menetluse võimaldamise ning terroriaktide tõkestamise, avastamise, uurimise ja nende eest vastutusele võtmise seisukohast proportsionaalne.

3. JÄRELHINDAMISE, SIDUSRÜHMADEGA KONSULTEERIMISE JA MÕJU HINDAMISE TULEMUSED

3.1. Konsulteerimine sidusrühmadega

Käesolevat seadusandlikku ettepanekut ette valmistades konsulteeris komisjon kõigi asjaomaste sidusrühmadega, et saada aru nende seisukohtadest ja kaaluda võimalusi edasiseks tegutsemiseks. Komisjon korraldas avaliku konsultatsiooni seoses meetmetega, millega võidelda ebaseadusliku sisu vastu, ja sai 8 961 vastust. 8 749 vastajat olid eraisikud, 172 organisatsioonid, 10 avaliku sektori asutused ja 30 kuulus muudesse vastajate kategooriatesse. Samal ajal korraldati ebaseadusliku veebisisu teemal Eurobaromeetri uuring, mille käigus küsitleti 33 500 juhuslikult valitud ELi elanikku. Samuti konsulteeris komisjon 2018. aasta mais ja juunis liikmesriikide ametiasutuste ja veebimajutusteenuse pakkujatega seoses erimeetmetega terroristliku veebisisu vastu võitlemiseks.

Valdav enamus sidusrühmade esindajaid leidis, et terroristlik veebisisu on tõsine ühiskondlik probleem, mis mõjutab internetikasutajaid ja veebimajutusteenuse pakkujate ärimudeleid. Üldisemalt leidis 65 % Eurobaromeetri[4] uuringule vastanuist, et internet ei ole kasutajate jaoks ohutu, ja 90 % vastanuist pidas oluliseks piirata ebaseadusliku veebisisu levitamist. Liikmesriikidega konsulteerides selgus, et ehkki vabatahtlikud kokkulepped annavad tulemusi, näevad paljud vajadust terroristliku sisu kohta käivate siduvate nõuete järele – samal meelel oldi ka Euroopa Ülemkogu 2018. aasta juunikuistes järeldustes. Ehkki üldiselt pooldasid veebimajutusteenuse pakkujad vabatahtlike meetmete jätkamist, tõid nad välja liidus tekkiva õigusliku killustatuse võimaliku negatiivse mõju.

Samuti märkisid paljud sidusrühmad vajadust tagada, et vastukaaluks mis tahes reguleerimismeetmetele sisu eemaldamise kohta, eriti ennetavatele meetmetele ja rangetele tähtaegadele, tuleks võtta meetmed põhiõiguste, eriti sõnavabaduse kaitseks. Sidusrühmad tõid välja hulga vajalikke meetmeid seosed läbipaistvuse ja vastutusega ning vajadusega inimese tehtava kontrolli järele automaatsete vahendite kasutuselevõtu korral.

3.2. Mõjuhinnang

Õiguskontrollikomitee andis mõjuhinnangu kohta reservatsioonidega positiivse arvamuse ja esitas mitu täiustamissoovitust[5]. Selle arvamuse tulemusena muudeti mõjuhinnangu aruannet, et võtta arvesse õiguskontrollikomitee peamisi märkusi: tähelepanu keskmesse võeti terroristlik sisu, rõhutades samal ajal täiendavalt mõju digitaalse ühtse turu toimimisele, ning põhjalikumalt analüüsiti põhiõigustele avalduvat mõju ja erinevate variantide raames välja pakutud kaitsemeetmete toimimist.

Eeldatakse, et kui täiendavaid meetmeid ei võeta, jätkatakse vabatahtlikke meetmeid, millel on terroristliku veebisisu vähendamisele teatav mõju. Ent on ebatõenäoline, et vabatahtlikke meetmeid võtavad kõik sellise sisuga kokku puutuvad veebimajutusteenuse pakkujad, ja eelduste kohaselt suureneb õiguslik killustatus, mis paneb uued tõkked piiriülesele teenuste pakkumisele. Lisaks lähtestsenaariumile vaeti kolme peamist poliitikavarianti, millest igaühe

[4] Eurobaromeetri uuring 469 ebaseadusliku veebisisu kohta, juuni 2018.

[5] Dokument õiguskontrollikomitee dokumendiregistris.

tulemuslikkuse tase mõjuhinnangus sätestatud eesmärkide ja üldise poliitikaeesmärgi, see tähendab terroristliku veebisisu vähendamise käsitlemisel oli eelneva omast suurem.

Kõigi kolme variandi kohustuste puhul keskenduti veebimajutusteenuse pakkujatele asukohaga ELis ja kolmandates riikides (isikuline kohaldamisala), kui nad osutavad oma teenuseid liidus (geograafiline kohaldamisala). Võttes arvesse probleemi olemust ja vajadust vältida väiksemate platvormide kuritarvitamist, ei ole ühegi variandi puhul ette nähtud erandeid VKEdele. Kõigi variantide kohaselt peab veebimajutusteenuse pakkujal olema seaduslik esindaja ELis (see kehtib selliste ettevõtete puhul, kelle asukoht on väljaspool ELi), et tagada ELi õigusnormide täitmise tagamine. Kõigi variantide raames nähti ette, et liikmesriigid töötavad välja karistusmehhanismid.

Kõigi variantidega nähti ette luua uus, ühtlustatud süsteem eemaldamiskorralduste jaoks, mille riigi ametiasutused esitavad veebimajutusteenuse pakkujatele seoses terroristliku veebisisuga, ja nõue eemaldada selline sisu ühe tunni jooksul. Veebimajutusteenuse pakkujal ei oleks ilmtingimata kohustust neid korraldusi hinnata ja nendega seoses oleks võimalik pöörduda kohtusse.

Kõigi kolme variandi ühisosa on kaitsemeetmed, eriti kaebemenetlused ja tõhusad õiguskaitsevahendid, sealhulgas võimalus pöörduda kohtusse, samuti muud sätted, et vältida sellise sisu ekslikku eemaldamist, mis ei ole terroristlik, ja tagada samal ajal kooskõla põhiõigustega. Lisaks sellele hõlmavad kõik variandid aruandekohustust avaliku läbipaistvuse vormis ning kahtlustatavatest kuritegudest teatamist liikmesriikidele, komisjonile ja ametiasutustele. Lisaks sellele nähakse ette, et riigi ametiasutused, veebimajutusteenuse pakkujad ja vajaduse korral Europol peavad tegema koostööd.

Kolme variandi peamised erinevused puudutavad terroristliku sisu määratlust, esildiste ühtlustatuse taset, ennetavate meetmete ulatust, liikmesriikide koordineerimiskohustust, samuti nõudeid andmete säilitamise kohta. Esimese variandi kohaselt piirduks materiaalne kohaldamisala sisuga, mida levitatakse eesmärgiga otseselt õhutada toime panema terroristlikku akti, mis on määratletud kitsalt, teise ja kolmanda valiku puhul aga kasutataks ulatuslikumat lähenemisviisi, hõlmates ka värbamist ja väljaõpet puudutavat materjali. Ennetavate meetmete vallas tuleks terroristliku veebisisuga kokku puutunud veebimajutusteenuse pakkujatel esimese variandi korral teha riskihindamine, ent ennetavad meetmed riski käsitlemiseks jääksid vabatahtlikuks. Teise variandi kohaselt peaksid veebimajutusteenuse pakkujad koostama tegevuskava, mis võib hõlmata automaatseid vahendeid juba eemaldatud sisu uuesti üleslaadimise takistamiseks. Kolmas variant hõlmab ulatuslikumaid ennetavaid meetmeid, millest tulenevalt terroristliku veebisisuga kokku puutunud teenusepakkujad peavad kindlaks tegema ka uue materjali. Kõigi variantide puhul oleksid ennetavate meetmete suhtes kehtivad nõuded proportsionaalsed terroristliku materjaliga kokkupuute taseme ja teenuseosutaja majandusliku suutlikkusega. Mis puudutab esildisi, siis esimese variandiga ei ühtlustataks nende suhtes kasutatavat lähenemisviisi, teise variandiga toimuks ühtlustamine Europoli puhul ja kolmanda variandi korral oleksid lisaks hõlmatud liikmesriikide esildised. Teise ja kolmanda variandi kohaselt oleks liikmesriikidel kohustus omavahel teavet jagada, koordineerida ja koostööd teha; kolmanda variandi puhul peaksid nad lisaks tagama, et nende pädevatel ametiasutustel oleks suutlikkus terroristliku veebisisu avastamiseks ja sellest teatamiseks. Samuti hõlmab kolmas variant andmete säilitamise nõuet, mis on kaitsemeede eksliku eemaldamise puhuks ja peab hõlbustama kriminaaluurimist.

Lisaks õigusnormidele nähti ette, et kõigi seadusandlike variantidega käiksid kaasas toetavad meetmed, ennekõike eesmärgiga lihtsustada erinevate riigi ametiasutuste koostööd omavahel

ja Europoliga ning koostööd veebimajutusteenuse pakkujatega, ja tugi teadus- ja arendustegevuse ning innovatsiooni vallas, et töötada välja ja võtta kasutusele tehnoloogilisi lahendusi. Pärast õigusakti vastuvõtmist võidakse kasutusele võtta ka täiendavad vahendid VKEde teadlikkuse suurendamiseks ja toetamiseks.

Mõjuhinnangu järeldus oli, et poliitikaeesmärgi saavutamiseks on vaja võtta teatavaid meetmeid. Terroristliku sisu kitsale määratlusele (esimene variant) tuleks eelistada sisu laia määratlust, mis hõlmaks kõige kahjulikumat materjali. Ennetavad kohustused, mis piirduksid terroristliku sisu uuesti üleslaadimise tõkestamisega (teine variant), ei oleks nii mõjusad kui uue terroristliku sisu avastamisega seotud kohustused (kolmas variant). Esildiste kohta käivad sätted peaksid hõlmama nii Europoli kui ka liikmesriikide esildisi (kolmas variant) ja mitte piirduma ainult Europoli esildistega (teine variant), kuna liikmesriikide esildised annavad olulise panuse üldistesse jõupingutustesse terroristliku veebisisu kättesaadavuse vähendamiseks. Nimetatud meetmed tuleks rakendada lisaks meetmetele, mis on kõigi variantide puhul ühised ja mille hulka kuuluvad kindlad meetmed kaitseks sisu eksliku eemaldamise eest.

3.3. Põhiõigused

Terroristide veebipropaganda püüab õhutada inimesi terrorirünnakuid toime panema, sealhulgas andes neile üksikasjalikud juhised selle kohta, kuidas võimalikult rohkem kahju teha. Tavaliselt avaldatakse pärast selliseid hirmutegusid uus propaganda, milles neid tegusid ülistatakse ja kutsutakse teisi üles sama eeskuju järgima. Käesolev määrus aitab kaitsta avalikku julgeolekut, piirates juurdepääsu terroristlikule sisule, mis propageerib põhiõiguste rikkumist ja kannustab seda tegema.

Ettepanek võib mõjutada mitut põhiõigust:

(a) sisuteenuse pakkuja õigused; õigus sõnavabadusele, õigus isikuandmete kaitsele, õigus era- ja perekonnaelu austamisele, mittediskrimineerimise põhimõte ja õigus tõhusale õiguskaitsevahendile;

(b) teenuse osutaja õigused; õigus ettevõtlusvabadusele; õigus tõhusale õiguskaitsevahendile;

(c) kõigi kodanike õigused; õigus sõna- ja teabevabadusele.

Võttes arvesse asjaomast õigustikku, hõlmab kavandatud määrus nende isikute õiguste kaitse tagamiseks asjakohaseid ja kindlaid kaitsemeetmeid.

Esimene element selles kontekstis on asjaolu, et määruses on kooskõlas direktiivis (EL) 2017/541 esitatud terroriakti määratlusega esitatud terroristliku veebisisu määratlus. Seda määratlust kohaldatakse eemaldamiskorralduste, esildiste ja ennetavate meetmete suhtes. Määratlusega on tagatud, et eemaldatakse ainult ebaseaduslik sisu, mis vastab seotud kuritegude üleliidulisele määratlusele. Lisaks sellele hõlmab määrus veebimajutusteenuse pakkujate üldiseid hoolsuskohustusi, mille kohaselt nende tegevus nende talletatava sisu suhtes peab olema hoolikas, proportsionaalne ja mittediskrimineeriv, eelkõige oma teenuste osutamise tingimusi rakendades, et vältida sellise sisu eemaldamist, mis ei ole terroristlik.

Täpsemalt on määrus kavandatud selleks, et tagada võetud meetmete proportsionaalsus põhiõiguste austamisega. Eemaldamiskorralduste puhul õigustab meetme ühe tunni pikkust tähtaega see, et pädev asutus hindab sisu (sealhulgas teeb vajaduse korral õiguslikku kontrolli). Lisaks piirduvad esildiste kohta käivad sätted käesolevas määruses nende esildistega, mille saadavad pädevad asutused ja liidu asutused, andes selgitusi selle kohta,

miks sisu võidakse pidada terroristlikuks. Ehkki esildises kirjeldatud sisu eemaldamise eest vastutab veebimajutusteenuse pakkuja, hõlbustab ülalnimetatud hindamine tehtavat otsust.

Ennetavate meetmete suhtes vastutab sisu kindlakstegemise, hindamise ja eemaldamise eest veebimajutusteenuse pakkuja, kes peab kehtestama kaitsemeetmed, tagamaks, et sisu ei eemaldata ekslikult, sealhulgas inimese tehtava kontrolli tulemusena, eriti juhul, kui konteksti on vaja täiendavalt selgitada. Peale selle, vastupidiselt lähtestsenaariumile, mille puhul kõige rohkem mõjutatud ettevõtted võtavad kasutusele automaatsed vahendid, ilma et selle suhtes tehtaks avalikku järelevalvet, tuleks meetmete väljatöötamise ja nende rakendamise kohta anda aru liikmesriikide pädevatele asutustele. See nõue vähendab eksliku eemaldamise ohtu nii nende ettevõtete jaoks, kes uusi vahendeid kasutusele võtavad, kui ka nende jaoks, kes neid juba kasutavad. Lisaks peavad veebimajutusteenuse pakkujad andma sisuteenuse pakkujate käsutusse kasutajasõbralikud kaebuste esitamise mehhanismid, mille kaudu nad saavad vaidlustada nende sisu eemaldamise otsuseid, ja avaldama üldsusele läbipaistvusaruanded.

Kui peaks juhtuma, et sisu ja sellega seotud andmed hoolimata neist kaitsemeetmetest ekslikult eemaldatakse, peavad veebimajutusteenuse pakkujad seda kuus kuud säilitama, et sisu oleks võimalik taastada, tagamaks kaebe- ja läbivaatamismenetluste tulemuslikkus ning kaitsmaks sõna- ja teabevabadust. Samal ajal aitab säilitamine kaasa ka õiguskaitsele. Veebimajutusteenuse pakkujad peavad kehtestama tehnilised ja korralduslikud kaitsemeetmed, millega tagatakse, et andmeid ei kasutata muudel eesmärkidel.

Kavandatud meetmed, eriti need, mis on seotud eemaldamiskorralduste, esildiste, ennetavate meetmete ja andmete säilitamisega, peaksid mitte ainult kaitsma internetikasutajaid terroristliku sisu eest, vaid aitama terroristliku veebisisu kättesaadavust vähendades samuti kaitsta kodanike õigust elule.

4. MÕJU EELARVELE

Määruse seadusandlik ettepanek ei mõjuta ELi eelarvet.

5. MUU TEAVE

5.1. Rakenduskavad ning järelevalve, hindamise ja aruandluse kord

Komisjon koostab [üks aasta pärast käesoleva määruse kohaldamise alguskuupäeva] käesoleva määruse väljundite, tulemuste ja mõju järelevalveks üksikasjaliku kava. Järelevalvekavas sätestatakse andmete ja muu vajaliku tõendusmaterjali kogumisel kasutatavad näitajad ja vahendid ning kogumise sagedus. Selles täpsustatakse, millised on komisjoni ja liikmesriikide ülesanded andmete ja muu tõendusmaterjali kogumisel ja analüüsimisel, et jälgida edusamme ja hinnata käesolevat määrust.

Koostatud järelevalvekava põhjal esitab komisjon kahe aasta jooksul pärast käesoleva määruse jõustumist aruande käesoleva määruse rakendamise kohta, mis tugineb ettevõtete avaldatud läbipaistvusaruannetele ja liikmesriikide esitatud teabele. Komisjon teeb hindamise mitte varem kui neli aastat pärast määruse jõustumist.

Tuginedes hindamise tulemustele, seahulgas teatavate lünkade või nõrkuste võimalikule püsimisele, ja võttes arvesse tehnoloogia arengut, hindab komisjon vajadust laiendada määruse kohaldamisala. Vajaduse korral esitab komisjon käesoleva määruse kohandamise ettepanekud.

Komisjon toetab määruse rakendamist, järelevalvet ja hindamist komisjoni eksperdirühma kaudu. Lisaks soodustab rühm koostööd veebimajutusteenuse pakkujate, õiguskaitseasutuste ja Europoli vahel, edendab terroristliku sisu avastamise ja eemaldamise alaste kogemuste ja teabe vahetamist ning sellealaseid meetodeid ja annab ekspertteavet selle kohta, kuidas muutub terroristide viis veebis tegutseda; vajaduse korral annab rühm ka nõu ja juhiseid sätete rakendamiseks.

Kavandatava määruse rakendamist peaksid hõlbustama mitu toetusmeedet. Nende hulgas on võimalus töötada Europoli raames välja platvorm esildiste ja eemaldamiskorralduste koordineerimise toetamiseks. ELi finantseeritud uuring selle kohta, kuidas terroristide tegutsemisviis muutub, suurendab kõigi asjaomaste sidusrühmade sellealaseid teadmisi ja teadlikkust. Lisaks sellele toetatakse programmi „Horisont 2020“ raames teadustegevust eesmärgiga töötada välja uut tehnoloogiat, sealhulgas automaattõkked, mis takistavad terroristliku sisu üleslaadimist. Lisaks sellele vaeb komisjon jätkuvalt võimalusi toetada ELi rahastamisvahendite kaudu pädevaid asutusi ja veebimajutusteenuse pakkujaid käesoleva määruse rakendamisel.

5.2. Ettepaneku sätete üksikasjalik selgitus

Artiklis 1 sätestatakse reguleerimisese, märkides, et määruses sätestatakse õigusnormid, et tõkestada veebimajutusteenuste kuritahtlikku kasutamist terroristliku veebisisu levitamiseks, sealhulgas veebimajutusteenuse pakkujate hoolsuskohustused ja meetmed, mille peavad võtma liikmesriigid. Samuti määratakse sellega kindlaks geograafiline kohaldamisala, mis hõlmab liidus teenuseid pakkuvaid veebimajutusteenuse pakkujaid olenemata sellest, kus on nende asukoht.

Artiklis 2 on esitatud ettepanekus kasutatud mõistete selgitused. Samuti on selles ennetaval eesmärgil esitatud terroristliku sisu määratlus, lähtudes terrorismivastase võitluse direktiivist, et hõlmata materjale ja teavet, mis õhutavad, julgustavad või toetavad terroriaktide toimepanemist või neile kaasaaitamist, annavad juhiseid selliste kuritegude toimepanekuks või propageerivad osalemist terrorirühmituste tegevuses.

Artiklis 3 sätestatakse hoolsuskohustused, mida veebimajutusteenuse pakkujad peavad täitma, kui nad võtavad meetmeid kooskõlas käesoleva määrusega, ja pidades ennekõike silmas seonduvaid põhiõiguseid. Artikliga nähakse ette, et veebimajutusteenuse pakkuja tingimustesse tuleb sisse viia asjakohased sätted ja et seejärel tuleb tagada nende kohaldamine.

Artikliga 4 pannakse liikmesriikidele kohustus anda pädevatele asutustele volitused teha eemaldamiskorraldusi ja kehtestatakse veebimajutusteenuse pakkujatele nõue eemaldada sisu ühe tunni jooksul pärast eemaldamiskorralduse saamist. Samuti sätestatakse selles eemaldamiskorralduse kohustuslik miinimumsisu ja menetlused, mille varal veebimajutusteenuse pakkujad annavad korralduse teinud asutusele tagasisidet ning teavitavad neid juhul, kui korraldust ei ole võimalik täita või kui on vaja täiendavaid selgitusi. Samuti pannakse sellega korralduse teinud asutusele kohustus teavitada selle liikmesriigi ennetavate meetmete eest vastutavat asutust, mille jurisdiktsiooni alla veebimajutusteenuse pakkuja kuulub.

Artiklis 5 sätestatakse veebimajutusteenuse pakkujatele nõue kehtestada meetmed, et hinnata kiiresti sisu, millele kas liikmesriigi pädeva asutuse või liidu asutuse tehtud esildises

viidatakse, kehtestamata siiski kohustust viidatud sisu eemaldada ja panemata tegutsemisele konkreetseid ajalisi piire. Samuti sätestatakse selles esildise kohustuslik miinimumsisu ja menetlused, mille varal veebimajutusteenuse pakkujad annavad esildise teinud asutusele tagasisidet ning küsivad selgitusi asutuselt, kes sisust teatas.

Artikliga 6 pannakse veebimajutusteenuse pakkujatele kohustus võtta vajaduse korral tulemuslikke ja proportsionaalseid ennetavaid meetmeid. Selles sätestatakse menetlus, millega tagatakse, et teatavad veebimajutusteenuse pakkujad (st need teenusepakkujad, kes on saanud lõplikuks muutunud eemaldamiskorralduse) võtavad vajaduse korral täiendavad ennetavad meetmed riski leevendamiseks ja vastavalt sellele, kuivõrd nende teenuste kaudu võib terroristliku sisuga kokku puutuda. Veebimajutusteenuse pakkuja peaks vajaolevate meetmete vallas tegema koostööd pädeva asutusega ja kui kokkulepet saavutada on võimatu, võib asutus veebimajutusteenuse pakkuja suhtes meetmeid kehtestada. Samuti sätestatakse artiklis asutuse otsuse läbivaatamise kord.

Artikliga 7 pannakse veebimajutusteenuse pakkujale kohustus säilitada eemaldatud sisu ja sellega seotud teavet läbivaatamismenetluse või uurimisega seotud eesmärkidel. Seda aega võidakse pikendada, et läbivaatamise saaks lõpule viia. Samuti pannake selle artikliga teenusepakkujatele kohustus kehtestada kaitsemeetmed, tagamaks, et säilitatavale sisule ja sellega seotud andmetele ei ole juurdepääsu ja neid ei töödelda muul eesmärgil.

Artikliga 8 kehtestatakse veebimajutusteenuse pakkujatele nõue selgitada, milliseid põhimõtteid nad terroristliku sisu levitamise vastu rakendavad, ja esitada iga-aastased läbipaistvusaruanded sellega seoses võetud meetmete kohta.

Artikliga 9 nähakse ette spetsiaalsed kaitsemeetmed seoses automaatsete vahendite kaudu ennetavate meetmete kasutamise ja rakendamisega, et tagada otsuste täpsus ja põhjendatus.

Artikliga 10 pannakse veebimajutusteenuse pakkujatele kohustus võtta kasutusele eemaldamiste, esildiste ja ennetavate meetmetega seotud kaebuste esitamise mehhanismid ja vaadata kõik kaebused kiiresti läbi.

Artikliga 11 kehtestatakse veebimajutusteenuse pakkujatele nõue teha teave eemaldamise kohta kättesaadavaks sisuteenuse pakkujale, välja arvatud juhul, kui pädev asutus nõuab teabe saladuses hoidmist avaliku julgeolekuga seotud põhjustel.

Artikliga 12 pannakse liikmesriikidele kohustus tagada, et pädevatel asutustel on piisav võimekus ja ressursid, et täita neile käesolevast määrusest tulenevad kohustused.

Artikliga 13 pannakse liikmesriikidele kohustus teha koostööd üksteisega ja vajaduse korral Europoliga, et vältida tegevuse dubleerimist ja uurimistesse sekkumist. Samuti nähakse selle artikliga liikmesriikidele ja veebimajutusteenuse pakkujatele ette võimalus kasutada spetsiaalseid (sh Europoli) vahendeid eemaldamiskorralduste ja esildiste töötlemiseks ja nende kohta tagasiside andmiseks ning koostööks ennetavate meetmete vallas. Samuti pannakse sellega liikmesriikidele kohustus seada sisse kohased sidekanalid, et tagada õigeaegne teabevahetus käesoleva määruse rakendamisel ja täitmise tagamisel. Samuti peavad veebimajutusteenuse pakkujad selle artikli kohaselt teavitama asjaomaseid asutusi, kui nad on teadlikud tõendusmaterjalist terroriaktide kohta terrorismivastast võitlust käsitleva direktiivi (EL) 2017/541 artikli 3 tähenduses.

Artikliga 14 nähakse ette, et nii veebimajutusteenuse pakkujad kui ka liikmesriigid loovad kontaktpunktid, et hõlbustada omavahelist suhtlust, eriti seoses esildiste ja eemaldamiskorraldustega.

Artikliga 15 kehtestatakse liikmesriikide jurisdiktsioon seoses kontrolliga ennetavate meetmete üle, karistuste kehtestamise ja järelevalvega.

Artikliga 16 kehtestatakse nõue, et veebimajutusteenuse pakkujad, kellel ei ole üksust mitte üheski liikmesriigis, kuid kes pakuvad liidus teenuseid, peavad määrama seadusliku esindaja liidus.

Artikliga 17 pannakse liikmesriikidele kohustus määrata asutused, kes teevad eemaldamiskorraldusi, annavad teada terroristlikust sisust, teevad järelevalvet ennetavate meetmete rakendamise üle ja tagavad määruse täitmise.

Artiklis 18 on sätestatud, et liikmesriigid peaksid ette nägema õigusnormid karistuste kohta, mida kohaldatakse kohustuste täitmata jätmise korral, ja kriteeriumid, mida liikmesriigid peavad arvesse võtma karistuste liiki ja suurust kindlaks määrates. Kuna eemaldamiskorralduses viidatud terroristliku sisu kiire eemaldamine on eriti oluline, tuleks kehtestada erinormid rahaliste karistuste kohta, mida kohaldatakse selle nõude süstemaatilise eiramise korral.

Artikliga 19 kehtestatakse kiirem ja paindlikum menetlus, et muuta delegeeritud õigusaktidega eemaldamiskorralduste jaoks kehtestatud vorme ja autenditud kanaleid nende esitamiseks.

Artikliga 20 kehtestatakse tingimused, mille alusel on komisjonil õigus võtta vastu delegeeritud õigusakte, et teha vormides ja eemaldamiskorraldustele esitatavates tehnilistes nõuetes vajalikke muudatusi.

Artikliga 21 pannakse liikmesriikidele kohustus koguda ja esitada määruse kohaldamisega seotud konkreetset teavet, et abistada komisjoni tema artiklis 23 sätestatud ülesannete täitmisel. Komisjon koostab käesoleva määruse väljundite, tulemuste ja mõju jälgimise üksikasjaliku kava.

Artiklis 22 sätestatakse, et komisjon esitab aruande käesoleva määruse rakendamise kohta kaks aastat pärast selle jõustumist.

Artiklis 23 sätestatakse, et komisjoni esitab aruande käesoleva määruse hindamise kohta mitte varem kui kolm aastat pärast selle jõustumist.

Artiklis 24 sätestatakse, et kavandatav määrus jõustub kahekümnendal päeval pärast selle avaldamist *Euroopa Liidu Teatajas* ja seda hakatakse kohaldama kuus kuud pärast selle jõustumise kuupäeva. Kavandatava tähtaja määramisel on arvesse võetud vajadust rakendusmeetmete järele, mööndes samas kavandatava määruse täieliku rakendamise pakilisust. Kuuekuine ülevõtmistähtaeg on kehtestatud eeldusel, et läbirääkimised edenevad kiiresti.

2018/0331 (COD)

Ettepanek:

EUROOPA PARLAMENDI JA NÕUKOGU MÄÄRUS

terroristliku veebisisu levitamise tõkestamise kohta

Euroopa Komisjoni panus juhtide kohtumisse,
mis toimub Salzburgis 19.–20. septembril 2018

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[6],

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.

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

[6] ELT C ..., ..., lk …

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,[7] 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.

5) Käesoleva määruse kohaldamine ei tohiks mõjutada direktiivi 2000/31/EÜ[8] 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.

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.

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, mis on pluralistliku demokraatliku ühiskonna üks põhialuseid 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

---

[7] 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).

[8] 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).

õigusi. See õigus hõlmab veebimajutusteenuse ja sisuteenuse pakkujate jaoks võimalust vaidlustada eemaldamiskorraldus selle liikmesriigi kohtus, kelle ametiasutus eemaldamiskorralduse tegi.

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[9] kasutatud terroriakti määratlusest. Arvestades, et tegeleda tuleb kõige kahjulikuma internetis esineva terroristliku propagandaga, peaks määratlus hõlmama materjale ja teavet, mis õhutab, julgustab või toetab terroriaktide toimepanemist või neile kaasaaitamist, annab juhiseid selliste kuritegude toimepanekuks või propageerib osalemist terrorirühmituse tegevuses. Selline teave 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, ajakirjanduslikul või teaduslikul eemärgil tuleks asjakohaselt kaitsta. Terroristlikuks sisuks ei tohiks pidada radikaalsete, poleemiliste või vastuoluliste seisukohtade väljendamist tundlike poliitiliste küsimuste üle peetavas avalikus mõttevahetuses.

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 talletatakse tema palvel ning talletatud teave tehakse kättesaadavaks kolmandatele isikutele, olenemata sellest, kas selline tegevus on oma olemuselt puhtalt tehniline, automaatne või passiivne. Selliste infoühiskonna teenuse pakkujate hulka kuuluvad näiteks sotsiaalmeediaplatvormid, videovoogedastuse teenused, video-, pildi- ja audiomaterjalide jagamise teenused, failivahetus- ja muud pilvteenused, niivõrd kui need teevad teabe kättesaadavaks kolmandatele isikutele ja veebisaitidele, kus kasutajad saavad kommenteerida või arvustusi postitada. 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

[9] 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).

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[10] artikli 17 lõike 1 punkti c tähenduses. Teisalt, kui teenust osutatakse lihtsalt selleks, et järgida Euroopa Parlamendi ja nõukogu määruses (EL) 2018/302[11] sätestatud diskrimineerimiskeeldu, ei saa seda üksnes kõnealusele asjaolule tuginedes käsitada tegevuse suunamisena teatavale territooriumile liidus.

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 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 kohtusasutuse. 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. Veebimajutusteenuse pakkuja otsustab ise, kas eemaldab kõnealuse sisu või blokeerib liidu kasutajate juurdepääsu sellele sisule.

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

[10] 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).

[11] 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).

kvalifitseeritud e-andmevahetusteenuseid vastavalt Euroopa Parlamendi ja nõukogu määrusele (EL) 910/2014[12].

15) Pädeva asutuse või Europoli esildis on vahend, millega saab veebimajutusteenuse pakkujale tulemuslikult ja kiiresti teada anda tema teenuse konkreetsest sisust. Lisaks eemaldamiskorraldustele peaks kasutusele jääma ka selline mehhanism, mis võimaldab juhtida veebimajutusteenuse pakkuja tähelepanu teabele, mida võib pidada terroristlikuks sisuks, et teenusepakkuja saaks vabatahtlikult kaaluda selle sisu vastavust oma tingimustele. 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[13] 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 kokkupuude terroristliku sisuga on vähene.

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

---

[12] 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).

[13] 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).

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, aga ka 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 pakkuja peaks igal aastal avaldama läbipaistvusaruande, mis sisaldab sisulist teavet terroristliku sisu avastamiseks, kindlakstegemiseks ja eemaldamiseks võetud meetmete kohta.

25) Kaebuste lahendamise menetlused on vajalik kaitsemeede sõna- ja teabevabadusega kaitstud infosisu eksliku kõrvaldamise eest. 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.

26) Euroopa Liidu lepingu artikli 19 ja Euroopa Liidu põhiõiguste harta artikli 47 kohane tõhus õiguskaitse eeldab, 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) Kui pädevad asutused teevad veebimajutusteenuse pakkujatele eemaldamiskorraldusi või saadavad esildisi, peaksid nad jagama teavet, koordineerima ja tegema koostööd omavahel ja vajaduse korral ka Europoliga, et vältida topelttööd ja võimalikku sekkumist uurimistesse. 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.

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, võivad liikmesriigid kasutada Europoli välja töötatud 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[14].

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 vahendid, mille abil saab elektrooniliselt esitada eemaldamiskorraldusi ja esildisi, ning nende kiireks töötlemiseks vajalikud tehnilised vahendid ja 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 veebimajutusteenuse pakkuja tagama, et kontaktpunkt on kättesaadav seitse päeva nädalas ööpäev läbi. Teave kontaktpunkti kohta peaks sisaldama teavet selle kohta,

[14] COM(2018) 225 (lõplik).

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. Kui eemaldamiskorralduse teeb mõni teine liikmesriik, peaksid selle ametiasutused sellest hoolimata saama tagada oma korralduste täitmise, kohaldades mittekaristuslikke sunnimeetmeid, näiteks karistusmakseid. Kui tegemist on veebimajutusteenuse pakkujaga, kellel puudub liidus tegevuskoht ja kes ei määra endale esindajat, peaks igal liikmesriigil olema võimalik määrata karistusi eeldusel, et järgitakse topeltkaristamise keeldu.

35) Veebimajutusteenuse pakkuja, kelle tegevuskoht ei ole liidus, peaks määrama kirjalikus vormis esindaja, et tagada käesoleva määruse järgimine ja sellest tulenevate kohustuste täitmine.

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 karistuste kohta õigusnormid ning vajaduse korral ka 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. 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[15] sätestatud põhimõtetega. Eelkõige selleks, et tagada võrdne osalemine delegeeritud õigusaktide ettevalmistamises, saavad Euroopa Parlament ja nõukogu kõik dokumendid liikmesriikide ekspertidega samal ajal ning nende ekspertidel on võimalus pidevalt osaleda komisjoni eksperdirühmade koosolekutel, kus arutatakse delegeeritud õigusaktide ettevalmistamist.

41) Liikmesriigid peaksid koguma teavet õigusnormide rakendamise kohta. Käesoleva määruse väljundite, tulemuste ja mõju jälgimiseks tuleks koostada üksikasjalik programm, millest lähtudes õigusakti hinnata.

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,

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

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.

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:

   (a) veebimajutusteenuse pakkuja tegevuskoht on liidus;

   (b) ühes või mitmes liikmesriigis on märkimisväärne arv kasutajaid;

   (c) tegevus on suunatud ühele või mitmele liikmesriigile;

(4) „terroriakt“ – direktiivi (EL) 2017/541 artikli 3 lõikes 1 määratletud kuriteod;

(5) „terroristlik sisu“ – teave, mis vastab ühele või mitmele järgmistest tingimustest:

   (a) õhutab või õigustab, muu hulgas ülistamise teel, terroriaktide sooritamist, põhjustades seega selliste aktide sooritamise ohu;

   (b) julgustab terroriaktidele kaasa aitama;

   (c) propageerib terrorirühmituse tegevust, eeskätt seeläbi, et julgustab osalema direktiivi (EL) 2017/541 artikli 2 lõikes 3 määratletud terrorirühmituses või sellist rühmitust toetama;

(d) 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.

II JAGU
TERRORISTLIKU VEEBISISU LEVITAMISE TÕKESTAMISE MEETMED

Artikkel 3
Hoolsuskohustus

1. Veebimajutusteenuse pakkuja võtab 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 pakkuja paneb oma tingimustesse kirja sätted terroristliku sisu levitamise tõkestamise kohta ja kohaldab neid.

Artikkel 4
Eemaldamiskorraldused

1. Pädeval asutusel on õigus teha otsus, 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;

(b) põhjused, miks asjaomast sisu peetakse terroristlikuks sisuks; sealjuures viidatakse vähemalt artikli 2 lõikes 5 loetletud terroristliku sisu kategooriatele;

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

(d) viide käesolevale määrusele kui eemaldamiskorralduse õiguslikule alusele;

(e) korralduse tegemise kuupäev ja ajatempel;

(f) teave veebimajutusteenuse pakkujale ja sisuteenuse pakkujale kättesaadavate õiguskaitsevahendite kohta;

(g) 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 üksikasjaliku põhjenduse, 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. Veebimajutusteenuse pakkuja kinnitab korralduse kättesaamist ja teatab pädevale asutusele ilma põhjendamatu viivituseta 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 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 vabatatlikuks 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 piisavalt üksikasjalikku teavet, sealhulgas põhjused, miks sisu peetakse terroristlikuks, URL ja vajaduse korral täiendav teave, 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 kiiremas korras 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 vajaduse korral 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 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. 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 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 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 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 [nelja] nädala jooksul alates kõnealuse otsuse tegemisest. 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 asjaomaste liidu asutuste koostöö

1. Liikmesriikide pädevad asutused jagavad eemaldamiskorralduste ja esildiste küsimustes teavet, koordineerivad ja teevad koostööd omavahel ning vajaduse korral asjaomaste 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. Liikmesriigid ja veebimajutusteenuse pakkujad võivad otsustada kasutada spetsiaalseid vahendeid, sealhulgas vajaduse korral asjaomaste 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 kuritegude uurimise ja nende eest süüdistuse esitamisega tegelevat pädevat asutust või artikli 14 lõike 2 kohaselt tegutsevat kontaktpunkti liikmesriigis, kus on tema peamine tegevuskoht või esindaja. Kahtluste korral võib veebimajutusteenuse pakkuja edastada selle teabe 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.

2. Kui veebimajutusteenuse pakkuja ei suuda esindajat määrata, kuulub jurisdiktsioon kõigile liikmesriikidele.

3. Kui teise liikmesriigi ametiasutus on teinud eemaldamiskorralduse vastavalt artikli 4 lõikele 1, on selle liikmesriigi pädevuses võtta vastavalt oma riigi õigusele sunnimeetmeid eemaldamiskorralduse täitmise tagamiseks.

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 *[kuus kuud pärast käesoleva määruse jõustumist]* teatavad liikmesriigid komisjonile lõikes 1 osutatud 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. Ettenähtud karistused peavad olema mõjusad, proportsionaalsed ja hoiatavad. Liikmesriigid teatavad kõnealustest õigusnormidest ja meetmetest komisjonile hiljemalt [*kuue 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 isiku varasemad rikkumised;

(d) vastutava juriidilise 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 aruande koostamiseks vajaliku teabe.

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 [*6 kuud pärast jõustumist*].

Käesolev määrus on tervikuna siduv ja vahetult kohaldatav kõikides liikmesriikides.

Brüssel,

Euroopa Parlamendi nimel	*Nõukogu nimel*
president	*eesistuja*