AANBEVELINGEN

AANBEVELING (EU) 2018/334 VAN DE COMMISSIE

van 1 maart 2018

over maatregelen om illegale online-inhoud effectief te bestrijden

DE EUROPESE COMMISSIE,

Gezien het Verdrag betreffende de werking van de Europese Unie, en met name artikel 292,

Overwegende hetgeen volgt:

(1) Het internet en dienstverleners die op het internet actief zijn, leveren een aanzienlijke bijdrage aan innovatie, economische groei en werkgelegenheid in de Unie. Veel van deze dienstverleners spelen in de digitale economie een essentiële rol: zij brengen bedrijven en burgers samen en faciliteren het publieke debat en het verspreiden en ontvangen van feitelijke informatie, meningen en ideeën. Van hun diensten wordt echter in bepaalde gevallen misbruik gemaakt door derden om online illegale activiteiten te verrichten, zoals het verspreiden van bepaalde vormen van informatie met betrekking tot terrorisme, seksueel kindermisbruik, illegale haatuitingen of inbreuken op de wetgeving inzake consumentenbescherming, hetgeen het vertrouwen van de gebruikers kan ondermijnen en het bedrijfsmodel van de dienstverleners kan schaden. In sommige gevallen kunnen de betrokken dienstverleners zelfs bepaalde voordelen behalen uit dergelijke activiteiten, bijvoorbeeld als gevolg van de beschikbaarheid van auteursrechtelijk beschermde inhoud zonder toestemming van de rechthebbenden.

(2) De aanwezigheid van illegale online-inhoud heeft sterk negatieve gevolgen voor gebruikers, voor andere getroffen burgers en bedrijven, en voor de samenleving als geheel. De aanbieders van onlinediensten hebben, gezien hun centrale rol en de technologische middelen en mogelijkheden die samenhangen met de diensten die zij leveren, een bijzondere maatschappelijke verantwoordelijkheid om bij te dragen tot de bestrijding van illegale inhoud die met gebruikmaking van hun diensten wordt verspreid.

(3) Aangezien het voor het beperken van de schade en van de verdere verspreiding vaak essentieel is dat de illegale inhoud snel wordt verwijderd of ontoegankelijk wordt gemaakt, houdt die verantwoordelijkheid ook in dat de betrokken dienstverleners snel moeten kunnen beslissen over mogelijke maatregelen tegen die inhoud. De verantwoordelijkheid van de dienstverleners houdt ook in dat zij doeltreffende en passende voorzorgsmaatregelen moeten nemen, met name om een zorgvuldige en evenredige werkwijze te garanderen en te voorkomen dat onbedoeld inhoud wordt verwijderd die niet illegaal is.

(4) Veel aanbieders van onlinediensten erkennen deze verantwoordelijkheid en handelen in overeenstemming daarmee. Op collectief niveau is veel vooruitgang geboekt met vrijwillige regelingen van allerlei aard, waaronder het EU-internetforum over terroristische inhoud op internet, de gedragscode tegen illegale haatuitingen op internet en het memorandum van overeenstemming over de verkoop van namaakgoederen. Desondanks is illegale online-inhoud nog steeds een ernstig probleem in de Unie.

(5) Uit bezorgdheid over een reeks terroristische aanslagen in de EU en de woekering van terroristische propaganda op internet verklaarde de Europese Raad van 22-23 juni 2017 te verwachten „dat de sector een eigen forum opzet en nieuwe technologie en instrumenten ontwikkelt waarmee inhoud die aanzet tot terroristische daden, beter automatisch kan worden opgespoord om vervolgens te worden verwijderd". Het Europees Parlement drong er in een resolutie van 15 juni 2017 bij de onlineplatforms op aan „krachtigere maatregelen te nemen om illegale en schadelijke inhoud online aan te pakken". Ook de ministers van de lidstaten hebben de bedrijven er in het kader van het EU-internetforum nogmaals toe opgeroepen een proactievere aanpak te hanteren om hun gebruikers tegen terroristische inhoud te beschermen. Wat intellectuele-eigendomsrechten betreft, heeft de Raad in zijn conclusies van 4 december 2014 over de handhaving van deze rechten de Commissie verzocht aandacht te schenken aan het gebruik van instrumenten die beschikbaar zijn om degenen die inbreuk maken op intellectuele-eigendomsrechten, op te sporen en aan de rol van bemiddelaars bij de ondersteuning van de strijd tegen inbreuken op de intellectuele-eigendomsrechten.

(6) Op 28 september 2017 heeft de Commissie haar goedkeuring gehecht aan een mededeling met richtsnoeren over de verantwoordelijkheden van aanbieders van onlinediensten ten aanzien van illegale online-inhoud ([1]). In die mededeling heeft de Commissie uiteengezet dat zij zou onderzoeken of aanvullende maatregelen nodig zijn, onder meer door de vooruitgang die met vrijwillige regelingen is geboekt, in het oog te houden. Deze aanbeveling is een vervolg op die mededeling, weerspiegelt het ambitieuze karakter daarvan en geeft er gevolg aan, terwijl terdege rekening wordt gehouden met en wordt voortgebouwd op de grote vooruitgang die met die vrijwillige regelingen is geboekt.

(7) In deze aanbeveling wordt erkend dat terdege rekening moet worden gehouden met de specifieke kenmerken van de bestrijding van verschillende soorten illegale online-inhoud en met de specifieke oplossingen die vereist kunnen zijn, onder meer via gerichte wetgevingsmaatregelen. De Commissie heeft bijvoorbeeld de noodzaak van zulke specifieke wetgevingsmaatregelen erkend in haar voorstel van 25 mei 2016 tot wijziging van Richtlijn 2010/13/EU van het Europees Parlement en de Raad ([2]) in het licht van een veranderende marktsituatie. Voorts heeft zij op 14 september 2016 een voorstel voor een richtlijn inzake auteursrechten in de digitale eengemaakte markt ([3]) goedgekeurd, dat als doel heeft bepaalde dienstverleners te verplichten om in samenwerking met rechthebbenden maatregelen te nemen om de werking van overeenkomsten met rechthebbenden voor het gebruik van hun werken of andere materialen te verzekeren, en om via samenwerking met de dienstenaanbieders te voorkomen dat op hun diensten door rechthebbenden aangewezen werken of andere materialen beschikbaar worden gesteld. Deze aanbeveling laat die wetgevingsmaatregelen en -voorstellen onverlet.

(8) Richtlijn 2000/31/EG van het Europees Parlement en de Raad ([4]) voorziet in vrijstelling van aansprakelijkheid waarop aanbieders van onlinediensten, waaronder hostingdiensten als bedoeld in artikel 14 van die richtlijn, onder bepaalde voorwaarden een beroep kunnen doen. Om voor de vrijstelling van aansprakelijkheid in aanmerking te komen, moeten aanbieders van hostingdiensten prompt handelen om illegale informatie die bij hen is opgeslagen, te verwijderen of ontoegankelijk te maken, zodra zij daadwerkelijk kennis hebben van die illegale informatie en, wat schadevergoedingsvorderingen betreft, zij kennis hebben verkregen van feiten of omstandigheden waaruit het onwettige karakter van de activiteiten of informatie duidelijk blijkt. Zij kunnen die kennis onder meer verkrijgen door middel van bij hen ingediende meldingen. Richtlijn 2000/31/EG vormt daarmee het uitgangspunt voor het uitwerken van procedures om illegale informatie te verwijderen en ontoegankelijk te maken. Die richtlijn voorziet ook in de mogelijkheid voor de lidstaten om van de betrokken dienstverleners te verlangen dat zij zorgvuldigheid in acht nemen ten aanzien van illegale inhoud die mogelijk bij hen is opgeslagen.

(9) Wanneer de lidstaten maatregelen nemen ten aanzien van illegale online-inhoud, dienen zij het oorsprongslandbeginsel, zoals in Richtlijn 2000/31/EG vastgelegd, te eerbiedigen. Derhalve mogen zij niet, om redenen die binnen het gecoördineerde gebied als omschreven in die richtlijn vallen, de vrijheid van in een andere lidstaat gevestigde dienstverleners om diensten van de informatiemaatschappij te verlenen, beperken, onder voorbehoud echter van de mogelijkheid van afwijkingen onder bepaalde in die richtlijn vastgestelde voorwaarden.

(10) Daarnaast zijn er verscheidene andere rechtshandelingen van de Unie die voorzien in een rechtskader met betrekking tot bepaalde soorten illegale inhoud die online beschikbaar zijn en verspreid worden. Met name vereist Richtlijn 2011/93/EU van het Europees Parlement en de Raad ([5]) dat de lidstaten maatregelen nemen om webpagina's die kinderpornografie bevatten of verspreiden, te verwijderen, en staat de richtlijn hen toe de toegang tot dergelijke webpagina's te blokkeren, mits bepaalde waarborgen worden geboden. Richtlijn (EU) 2017/541 van het Europees Parlement en de Raad ([6]), die uiterlijk op 8 september 2018 in nationale wetgeving moet zijn omgezet, bevat analoge bepalingen ten aanzien van online-inhoud waarin publiekelijk wordt opgeroepen tot het plegen van een terroristisch misdrijf. Richtlijn (EU) 2017/541 stelt ook minimumvoorschriften

([1]) COM(2017) 555 final van 28 september 2017.
([2]) Richtlijn 2010/13/EU van het Europees Parlement en de Raad van 10 maart 2010 betreffende de coördinatie van bepaalde wettelijke en bestuursrechtelijke bepalingen in de lidstaten inzake het aanbieden van audiovisuele mediadiensten (richtlijn audiovisuele mediadiensten) (PB L 95 van 15.4.2010, blz. 1). COM(2016) 287 final.
([3]) COM(2016) 593 final van 14 september 2016.
([4]) Richtlijn 2000/31/EG van het Europees Parlement en de Raad van 8 juni 2000 betreffende bepaalde juridische aspecten van de diensten van de informatiemaatschappij, met name de elektronische handel, in de interne markt (richtlijn inzake elektronische handel) (PB L 178 van 17.7.2000, blz. 1).
([5]) Richtlijn 2011/93/EU van het Europees Parlement en de Raad van 13 december 2011 ter bestrijding van seksueel misbruik en seksuele uitbuiting van kinderen en kinderpornografie, en ter vervanging van Kaderbesluit 2004/68/JBZ van de Raad (PB L 335 van 17.12.2011, blz. 1).
([6]) Richtlijn (EU) 2017/541 van het Europees Parlement en de Raad van 15 maart 2017 inzake terrorismebestrijding en ter vervanging van Kaderbesluit 2002/475/JBZ van de Raad en tot wijziging van Besluit 2005/671/JBZ van de Raad (PB L 88 van 31.3.2017, blz. 6).

vast voor de definitie van strafbare feiten op het gebied van terroristische misdrijven, misdrijven in verband met een terroristische groepering en misdrijven in verband met terroristische activiteiten. Uit hoofde van Richtlijn 2004/48/EG van het Europees Parlement en de Raad ([1]) kunnen de bevoegde rechterlijke instanties een bevel uitvaardigen tegen tussenpersonen wier diensten door derden worden gebruikt om inbreuk op een intellectuele-eigendomsrecht te maken.

(11) Met name gezien deze achtergrond hebben sommige lidstaten, naast de vrijwillige maatregelen die sommige aanbieders van onlinediensten hebben genomen, na de vaststelling van Richtlijn 2000/31/EG regels vastgesteld voor meldings- en actieprocedures. Andere lidstaten overwegen dergelijke regels vast te stellen. De desbetreffende mechanismen zijn over het algemeen bedoeld om het voor de meldende partij gemakkelijker te maken om inhoud die zij illegaal acht, te melden bij de hostingdienstverlener („melding"), op grond waarvan deze kan beslissen of hij al dan niet instemt met de beoordeling en bereid is de inhoud te verwijderen of ontoegankelijk te maken („actie"). De verschillen tussen de nationale regels op dit gebied worden steeds groter. Bijgevolg kunnen voor de betrokken dienstverleners verschillende wettelijke voorschriften gelden, die uiteenlopen wat betreft inhoud en toepassingsgebied.

(12) In het belang van de interne markt en met het oog op de effectiviteit van de bestrijding van illegale online-inhoud en het behoud van de evenwichtige aanpak die met Richtlijn 2000/31/EG wordt beoogd, moeten enkele belangrijke beginselen worden vastgesteld als leidraad voor het optreden van de lidstaten en van de betrokken dienstverleners op dit gebied.

(13) Deze beginselen moeten worden vastgesteld en toegepast met volledige inachtneming van de door de rechtsorde van de Unie beschermde grondrechten, met name de in het Handvest van de grondrechten van de Europese Unie (hierna het „Handvest" genoemd) gewaarborgde rechten. Bij de bestrijding van illegale online-inhoud moeten geschikte en solide waarborgen worden toegepast om de grondrechten van alle betrokkenen te beschermen. Deze rechten omvatten onder meer de vrijheid van meningsuiting, met inbegrip van de vrijheid om kennis te nemen en te geven van informatie, het recht op eerbiediging van het privéleven en het familie- en gezinsleven, het recht op bescherming van persoonsgegevens en het recht op een doeltreffende rechterlijke bescherming van de gebruikers van de betrokken diensten. De bedoelde grondrechten kunnen ook de vrijheid van ondernemerschap van aanbieders van hostingdiensten, met inbegrip van hun contractvrijheid, alsmede de rechten van het kind en het recht op bescherming van eigendom, met inbegrip van de intellectuele eigendom, de menselijke waardigheid en non-discriminatie van bepaalde andere betrokken partijen omvatten. In het bijzonder moeten besluiten van aanbieders van hostingdiensten om door hen opgeslagen inhoud te verwijderen of ontoegankelijk te maken, terdege rekening houden met de grondrechten en de rechtmatige belangen van de gebruikers ervan, alsook met de centrale rol die deze dienstverleners spelen bij het faciliteren van het publieke debat en de verspreiding en kennisneming van feiten, meningen en ideeën overeenkomstig het recht.

(14) In overeenstemming met de horizontale aanpak die ten grondslag ligt aan de vrijstelling van aansprakelijkheid als bedoeld in artikel 14 van Richtlijn 2000/31/EG, dient deze aanbeveling te worden toegepast op alle soorten inhoud die strijdig zijn met het recht van de Unie of van de lidstaten, ongeacht het precieze onderwerp of de precieze aard van dit recht. Het volstaat om rekening te houden met het recht van de lidstaten die betrokken zijn bij de dienstverlening in kwestie, met name dat van de lidstaten op het grondgebied waarvan de aanbieder van de hostingdienst gevestigd is of waar de diensten worden verricht. Bij de toepassing van deze aanbeveling moet bovendien terdege rekening worden gehouden met de ernst en vormen van de schade die illegale inhoud kan aanrichten, een overweging die nauw dient samen te hangen met de snelheid van de te ondernemen actie die redelijkerwijs van aanbieders van hostingdiensten kan worden verwacht, waarbij in voorkomend geval rekening moet worden gehouden met de stand van de ontwikkeling en het mogelijke gebruik van technologieën. Ook moet terdege rekening worden gehouden met relevante verschillen die kunnen bestaan tussen verschillende soorten illegale inhoud en de te ondernemen actie om deze te bestrijden.

(15) Aanbieders van hostingdiensten spelen een bijzonder belangrijke rol bij de bestrijding van illegale online-inhoud, aangezien zij door hun gebruikers verstrekte informatie op hun verzoek opslaan en andere gebruikers toegang daartoe verlenen, vaak op grote schaal. Deze aanbeveling heeft dan ook in de eerste plaats betrekking op de activiteiten en verantwoordelijkheden van deze aanbieders. In voorkomend geval kunnen de aanbevelingen ook van overeenkomstige toepassing zijn op andere betrokken aanbieders van onlinediensten. Het doel van deze aanbeveling is het aanpakken van risico's in verband met illegale online-inhoud die consumenten in de Unie treffen. Zij heeft daarom betrekking op de activiteiten van alle aanbieders van hostingdiensten, ongeacht of zij zijn gevestigd in de Unie of in een derde land, voor zover hun activiteiten zijn gericht op consumenten die in de Unie wonen.

(16) Mechanismen voor het melden van illegaal geachte inhoud aan aanbieders van hostingdiensten zijn een belangrijk middel voor de bestrijding van illegale online-inhoud. Zulke mechanismen moeten het voor alle personen en

([1]) Richtlijn 2004/48/EG van het Europees Parlement en de Raad van 29 april 2004 betreffende de handhaving van intellectuele-eigendomsrechten (PB L 157 van 30.4.2004, blz. 45).

entiteiten gemakkelijker maken om illegale online-inhoud te melden. Deze mechanismen moeten dan ook voor iedereen gemakkelijk toegankelijk en eenvoudig te gebruiken zijn. Aanbieders van hostingdiensten moeten echter flexibel blijven, bijvoorbeeld wat betreft de vorm van de melding en de daarvoor te gebruiken technologie, zodat efficiënte oplossingen mogelijk zijn en een onevenredige belasting voor de melders wordt vermeden.

(17) Volgens de jurisprudentie van het Hof van Justitie met betrekking tot artikel 14 van Richtlijn 2000/31/EG moeten meldingen voldoende nauwkeurig zijn en naar behoren onderbouwd, zodat de aanbieder van hostingdiensten die de melding ontvangt, een gemotiveerd en zorgvuldig besluit kan nemen over het aan de melding te geven gevolg. Er moet daarom zo veel mogelijk voor worden gezorgd dat aan deze norm wordt voldaan. Of echter een ontvangen melding al dan niet leidt tot kennis of besef in de zin van artikel 14 van Richtlijn 2000/31/EG, moet worden beoordeeld in het licht van de specifieke kenmerken van het individuele geval, waarbij in aanmerking moet worden genomen dat die kennis of dat besef ook kan worden verkregen op andere manieren dan door een melding.

(18) De aanbieder van hostingdiensten hoeft doorgaans niet over de contactgegevens van de melder te beschikken om een gemotiveerd en zorgvuldig besluit te kunnen nemen over het aan de melding te geven gevolg. Het verplicht stellen van het verstrekken van contactgegevens bij een melding zou een obstakel vormen voor het indienen van meldingen. Om feedback te kunnen geven op de melding, moet de aanbieder van hostingdiensten echter wel over de contactgegevens beschikken. Het moet voor de melder bijgevolg wel mogelijk, maar niet verplicht zijn om zijn contactgegevens te verstrekken.

(19) Om de transparantie en de nauwkeurigheid van de meldings- en actiemechanismen te vergroten en het waar nodig mogelijk te maken verhaal te zoeken, zouden aanbieders van hostingdiensten, indien zij beschikken over de contactgegevens van melders en/of aanbieders van inhoud, de betrokkenen tijdig en correct moeten inlichten over de maatregelen die in het kader van de genoemde mechanismen zijn getroffen. Dat geldt met name als is besloten om de betrokken inhoud te verwijderen of ontoegankelijk te maken. De te verstrekken informatie moet evenredig zijn, in die zin dat zij in overeenstemming moet zijn met de beweringen in de melding of tegenmelding en tegelijkertijd passende en flexibele oplossingen mogelijk moet maken, zonder dat dit leidt tot een onredelijke last voor de melders of aanbieders.

(20) Met het oog op transparantie en billijkheid en om te voorkomen dat inhoud die niet illegaal is, onbedoeld wordt verwijderd, moeten aanbieders van inhoud in principe altijd worden ingelicht over het besluit om de op hun verzoek opgeslagen inhoud te verwijderen of ontoegankelijk te maken, en in de gelegenheid worden gesteld dat besluit aan te vechten door middel van een tegenmelding. Het doel daarvan kan zijn dat het besluit wordt herroepen, ongeacht of het is genomen naar aanleiding van een melding of een doorverwijzing of van een proactieve maatregel van de aanbieder van hostingdiensten.

(21) Gelet echter op de aard van de betrokken inhoud, het doel van een dergelijke tegenmelding en de extra lasten voor de aanbieders van hostingdiensten is er geen reden om aan te bevelen dat dergelijke informatie wordt verstrekt over het besluit en de mogelijkheid dit aan te vechten, wanneer duidelijk is dat de betrokken inhoud illegaal is en samenhangt met ernstige strafbare feiten die een bedreiging voor het leven of de veiligheid van personen inhouden, zoals bedoeld in Richtlijn (EU) 2017/541 en Richtlijn 2011/93/EU. Bovendien kan het in bepaalde gevallen om redenen van openbare orde en openbare veiligheid, en met name om redenen die verband houden met het voorkomen, onderzoeken, opsporen en vervolgen van strafbare feiten, gerechtvaardigd zijn dat dergelijke informatie niet rechtstreeks aan de betrokken aanbieder van inhoud wordt verstrekt. Aanbieders van hostingdiensten dienen dus geen informatie te verstrekken wanneer een bevoegde autoriteit hen heeft verzocht dat niet te doen, om redenen van openbare orde en openbare veiligheid, zolang die autoriteit om die redenen verzoekt die informatie niet te verstrekken. Voor zover dit een beperking inhoudt van het recht om in kennis te worden gesteld van de verwerking van persoonsgegevens, moet worden voldaan aan de voorwaarden van Verordening (EU) 2016/679 van het Europees Parlement en de Raad ([1]).

(22) Meldings- en actiemechanismen mogen in geen geval afbreuk doen aan het recht van de betrokken partijen om overeenkomstig het toepasselijke recht een gerechtelijke procedure in te leiden ten aanzien van illegaal geachte inhoud of maatregelen die aanbieders van hostingdiensten in dit verband nemen. Mechanismen voor buitengerechtelijke geschillenbeslechting kunnen in dit verband een belangrijke aanvulling vormen op gerechtelijke procedures, met name als zij een doeltreffende, betaalbare en snelle beslechting van dergelijke geschillen mogelijk maken. Buitengerechtelijke geschillenbeslechting moet derhalve worden aangemoedigd, mits de betrokken regelingen aan bepaalde normen voldoen: met name moet de billijkheid van de rechtsgang in acht worden genomen, moeten de partijen de mogelijkheid behouden de zaak voor de rechter te brengen en moet misbruik worden voorkomen.

([1]) Verordening (EU) 2016/679 van het Europees Parlement en de Raad van 27 april 2016 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens en tot intrekking van Richtlijn 95/46/EG (algemene verordening gegevensbescherming) (PB L 119 van 4.5.2016, blz. 1).

(23) Om de effectiviteit van de meldings- en actiemechanismen en andere activiteiten van aanbieders van hostingdiensten ten aanzien van illegaal geachte inhoud beter te kunnen beoordelen en ervoor te zorgen dat verantwoording wordt afgelegd, moet ten opzichte van het publiek transparant worden gehandeld. Aanbieders van hostingdiensten moeten daarom regelmatig verslag uitbrengen over deze mechanismen en andere activiteiten. De verslagen moeten zo volledig en gedetailleerd zijn dat een goed inzicht kan worden verkregen. De aanbieders moeten ook vooraf in hun contractvoorwaarden duidelijkheid bieden over hun beleid op het gebied van het verwijderen of ontoegankelijk maken van inhoud die bij hen is opgeslagen, met inbegrip van illegale inhoud.

(24) Naast meldings- en actiemechanismen kunnen ook evenredige en specifieke proactieve maatregelen die aanbieders van hostingdiensten, al dan niet op geautomatiseerde wijze, op basis van vrijwilligheid nemen, een belangrijk middel zijn in de strijd tegen illegale online-inhoud, onverminderd artikel 15, lid 1, van Richtlijn 2000/31/EG. Bij dergelijke proactieve maatregelen moet rekening worden gehouden met de situatie van aanbieders van hostingdiensten die door hun omvang of de schaal waarop zij opereren, slechts over beperkte middelen en deskundigheid beschikken, en met de noodzaak van effectieve en passende waarborgen bij dergelijke maatregelen.

(25) Dergelijke proactieve maatregelen kunnen in het bijzonder gepast zijn wanneer het illegale karakter van de inhoud reeds is vastgesteld of wanneer de aard van de inhoud zodanig is dat de context niet van wezenlijk belang is. Ook de aard, de schaal en het doel van de beoogde maatregelen kunnen van belang zijn, evenals de aard van de betrokken inhoud, de vraag of de inhoud is gemeld door de rechtshandhavingsautoriteiten of Europol, en of ten aanzien van de inhoud reeds actie is ondernomen omdat deze illegaal wordt geacht. In het bijzonder met betrekking tot materiaal in verband met seksueel kindermisbruik zouden aanbieders van hostingdiensten proactieve maatregelen moeten nemen om dergelijk materiaal op te sporen en de verspreiding ervan te voorkomen, overeenkomstig de verbintenissen die zijn aangegaan in het kader van de wereldwijde alliantie tegen seksuele uitbuiting van kinderen via het internet.

(26) In dit verband heeft de Commissie in haar mededeling van 28 september 2017 over de bestrijding van illegale online-inhoud haar standpunt uiteengezet dat het nemen van vrijwillige proactieve maatregelen er niet automatisch toe leidt dat de betrokken aanbieder van hostingdiensten het voordeel verliest dat voortvloeit uit de bij artikel 14 van Richtlijn 2000/31/EG voorziene vrijstelling van aansprakelijkheid.

(27) Het is van essentieel belang dat voor alle maatregelen ter bestrijding van illegale online-inhoud doeltreffende en passende garanties gelden, die ervoor zorgen dat aanbieders van hostingdiensten zorgvuldig en evenredig handelen bij de vaststelling en handhaving van hun beleid ten aanzien van inhoud die zij opslaan, met inbegrip van illegale inhoud, zodat er in het bijzonder voor zorg wordt gedragen dat gebruikers online vrijelijk kennis kunnen nemen en geven van informatie overeenkomstig het toepasselijk recht. Naast de waarborgen die zijn opgenomen in de toepasselijke wetgeving inzake bijvoorbeeld de bescherming van persoonsgegevens, moet worden voorzien in bepaalde voorzorgsmaatregelen, met name menselijk toezicht en menselijke verificatie, die waar nodig ook op geautomatiseerde middelen moeten worden toegepast, teneinde onbedoelde en onjuiste besluiten te voorkomen.

(28) Bij de bestrijding van illegale online-inhoud moet een vlotte, effectieve en passende samenwerking tussen bevoegde autoriteiten en aanbieders van hostingdiensten worden gewaarborgd. Bij die samenwerking kan bijstand van Europol van nut zijn, bijvoorbeeld wanneer het gaat om de bestrijding van terrorisme en seksueel misbruik en seksuele uitbuiting van kinderen, kinderpornografie en het benaderen van kinderen voor seksuele doeleinden. Teneinde deze samenwerking te faciliteren, moeten lidstaten en aanbieders van hostingdiensten contactpunten aanwijzen en moeten procedures worden vastgesteld om door die autoriteiten ingediende meldingen met voorrang te behandelen en eraan een passende mate van zekerheid over de juistheid ervan toe te kennen, rekening houdend met de specifieke deskundigheid en de taken van die autoriteiten. Met het oog op de doeltreffende bestrijding van bepaalde bijzonder ernstige strafbare feiten, zoals de feiten bedoeld in Richtlijn (EU) 2017/541 en Richtlijn 2011/93/EU, die onder de aandacht van aanbieders van hostingdiensten kunnen komen bij het uitvoeren van hun activiteiten, moeten de lidstaten worden aangemoedigd gebruik te maken van de in artikel 15, lid 2, van Richtlijn 2000/31/EG vervatte mogelijkheid om wettelijke rapportageverplichtingen in te stellen overeenkomstig het toepasselijk recht, met name Verordening (EU) 2016/679.

(29) Naast de bevoegde autoriteiten kunnen ook bepaalde personen of entiteiten, waaronder niet-gouvernementele organisaties en brancheverenigingen, beschikken over specifieke expertise en bereid zijn op vrijwillige basis bepaalde verantwoordelijkheden op zich te nemen met betrekking tot de bestrijding van illegale online-inhoud. In het licht van de toegevoegde waarde die deze „betrouwbare flaggers" bieden en de soms grote aantallen meldingen waarom het gaat, dient de samenwerking tussen hen en de aanbieders van hostingdiensten te worden aangemoedigd, in het bijzonder door de meldingen die zij indienen, eveneens prioritair te behandelen en eraan

een passende mate van zekerheid over hun juistheid toe te kennen. Gezien hun bijzondere status moet die samenwerking echter uitsluitend openstaan voor personen en entiteiten die de waarden eerbiedigen waarop de Unie is gegrondvest, zoals neergelegd in artikel 2 van het Verdrag betreffende de Europese Unie, en die voldoen aan bepaalde voorwaarden die duidelijk en objectief moeten zijn en openbaar moeten worden gemaakt.

(30) De bestrijding van illegale online-inhoud vereist een integrale aanpak, aangezien dergelijke inhoud zich vaak gemakkelijk verplaatst naar andere aanbieders van hostingdiensten en doorgaans gebruikmaakt van de zwakste schakels in de keten. Samenwerking, met name de uitwisseling van ervaringen, technologische oplossingen en beste praktijken op vrijwillige basis, is derhalve essentieel. Die samenwerking is vooral belangrijk voor aanbieders van hostingdiensten die door hun omvang of de schaal waarop zij opereren, slechts over beperkte middelen en deskundigheid beschikken.

(31) Terrorisme gaat gepaard met onrechtmatig en willekeurig gebruik van geweld en intimidatie jegens burgers. Terroristen maken in toenemende mate gebruik van het internet voor het verspreiden van terroristische propaganda en passen vaak geavanceerde methoden toe om een snelle en brede verspreiding te garanderen. Hoewel er vooruitgang is geboekt, met name in de context van het EU-internetforum, is het nog steeds dringend noodzakelijk om sneller en doeltreffender te reageren op terroristische online-inhoud. Ook moeten de aanbieders van hostingdiensten die aan het EU-internetforum deelnemen, ten volle hun belofte nakomen om voor doeltreffende en volledige rapportage te zorgen.

(32) Gezien de specifieke kenmerken van de bestrijding van terroristische online-inhoud moeten de aanbevelingen voor de bestrijding van illegale inhoud in het algemeen worden aangevuld met aanbevelingen die specifiek betrekking hebben op de bestrijding van terroristische online-inhoud. Verdere uitwerking en consolidatie van de in het kader van het EU-internetforum ondernomen werkzaamheden is daarvoor noodzakelijk.

(33) Gelet op de zeer ernstige risico's van terroristische inhoud en de centrale rol van de aanbieders van hostingdiensten bij de verspreiding van deze inhoud moeten de aanbieders van hostingdiensten alle redelijke maatregelen nemen om te verzekeren dat terroristische inhoud niet wordt doorgelaten en hosting ervan zo mogelijk wordt voorkomen, voor zover zij zelf hun contractvoorwaarden kunnen vaststellen en handhaven, en met inachtneming van doeltreffende en passende waarborgen, zulks onverminderd het bepaalde in artikel 14 van Richtlijn 2000/31/EG.

(34) Een belangrijk onderdeel van die maatregelen is de samenwerking met de bevoegde autoriteiten en Europol op het gebied van doorverwijzingen naar hostingdiensten. Doorverwijzingen zijn meldingen met een speciale vorm die is aangepast aan de bijzondere kenmerken van de bestrijding van terroristische inhoud. De bevoegde autoriteiten en Europol moeten aan doorverwijzingen een verzoek kunnen toevoegen om inhoud die zij terroristisch achten, te verwijderen of ontoegankelijk te maken, onder verwijzing naar de toepasselijke wetgeving of de contractvoorwaarden van de betrokken aanbieder van hostingdiensten. De procedure voor doorverwijzingen moet bestaan naast de mechanismen voor de melding van illegale inhoud door onder meer betrouwbare flaggers, die ook kunnen worden gebruikt voor het melden van terroristisch geachte inhoud.

(35) Aangezien terroristische inhoud doorgaans de meeste schade aanricht in het eerste uur na het verschijnen op internet, en gezien de specifieke deskundigheid en verantwoordelijkheden van de bevoegde autoriteiten en Europol, moeten doorverwijzingen in het algemeen binnen een uur worden getoetst en, indien nodig, een gevolg krijgen.

(36) De maatregelen tegen terroristische inhoud moeten evenredig, specifiek en proactief zijn. Dat wil zeggen dat ook geautomatiseerde middelen moeten kunnen worden ingezet om terroristische inhoud snel op te sporen, te identificeren en te verwijderen of ontoegankelijk te maken, en ervoor te zorgen dat die inhoud niet opnieuw op het internet verschijnt, onverminderd artikel 15, lid 1, van Richtlijn 2000/31/EG. In dit verband moet rekening worden gehouden met de noodzaak dat deze maatregelen gepaard gaan met adequate en effectieve waarborgen, die met name zijn opgenomen in hoofdstuk II van deze aanbeveling.

(37) Samenwerking, zowel tussen aanbieders van hostingdiensten onderling als met de bevoegde autoriteiten, is voor de bestrijding van terroristische online-inhoud van het allergrootste belang. Met name kunnen technologische hulpmiddelen om inhoud geautomatiseerd op te sporen, zoals de databank met hashcodes, nuttig zijn om te voorkomen dat terroristische inhoud via verschillende hostingdiensten wordt verspreid. Deze vorm van samenwerking en het ontwikkelen, toepassen en delen van dergelijke technologische hulpmiddelen moeten worden aangemoedigd, en waar nuttig moet daarbij gebruik worden gemaakt van de expertise van Europol. Deze gezamenlijke inspanningen zijn met name belangrijk om aanbieders van hostingdiensten die door hun omvang of de schaal waarop zij opereren, slechts over beperkte middelen en deskundigheid beschikken, in staat te stellen, zoals hierbij aanbevolen, snel en doeltreffend te reageren op meldingen en doorverwijzingen en proactieve maatregelen te nemen.

(38) Aan deze gezamenlijke inspanningen moeten zo veel mogelijk relevante aanbieders van hostingdiensten meewerken en alle deelnemende aanbieders van hostingdiensten moeten helpen bij het optimaliseren en maximaliseren van het gebruik van deze hulpmiddelen. Werkafspraken tussen alle betrokken partijen, waaronder indien nodig ook Europol, moeten worden aangemoedigd, aangezien zulke afspraken tot een consistente en doeltreffende aanpak kunnen bijdragen en de uitwisseling van ervaringen en expertise mogelijk maken.

(39) Om te waarborgen dat het grondrecht op de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en het vrije verkeer van persoonsgegevens worden gerespecteerd, moet de verwerking van persoonsgegevens bij alle maatregelen ter uitvoering van deze aanbeveling volledig in overeenstemming zijn met de gegevensbeschermingsregels, en met name met Verordening (EU) 2016/679 en Richtlijn (EU) 2016/680 van het Europees Parlement en de Raad ([1]). De bevoegde toezichthoudende autoriteiten moeten daarop toezien.

(40) Deze aanbeveling is in overeenstemming met de grondrechten en de beginselen die met name in het Handvest zijn erkend. Deze aanbeveling moet met name waarborgen dat de artikelen 1, 7, 8, 10, 11, 16, 17, 21, 24 en 47 van het Handvest ten volle worden geëerbiedigd.

(41) De Commissie is voornemens alle maatregelen die naar aanleiding van deze aanbeveling worden genomen, nauwlettend te monitoren. Lidstaten en aanbieders van hostingdiensten moeten derhalve bereid zijn om de Commissie desgevraagd alle relevante informatie te verstrekken die zij redelijkerwijs kunnen worden geacht te verstrekken met het oog op die monitoring. Aan de hand van de ontvangen informatie en alle andere beschikbare informatie, inclusief verslagen op basis van de verschillende vrijwillige regelingen, zal de Commissie het aan deze aanbeveling gegeven gevolg beoordelen en nagaan of aanvullende maatregelen nodig zijn, zoals voorstellen voor bindende rechtshandelingen van de Unie. Gezien de specifieke kenmerken en de urgentie van de bestrijding van terroristische online-inhoud moeten de monitoring en beoordeling daarvan op basis van gedetailleerde informatie en bijzonder snel worden verricht, namelijk binnen drie maanden na de bekendmaking van deze aanbeveling, terwijl voor andere illegale inhoud zes maanden na de bekendmaking een passende termijn is,

HEEFT DE VOLGENDE AANBEVELING VASTGESTELD:

HOOFDSTUK I

Doel en terminologie

1. Ten aanzien van inhoud die door aanbieders van inhoud wordt verstrekt en op hun verzoek door aanbieders van hostingdiensten wordt opgeslagen, worden de lidstaten en de aanbieders van hostingdiensten aangemoedigd doeltreffende, passende en evenredige maatregelen te nemen ter bestrijding van illegale online-inhoud, in overeenstemming met de in deze aanbeveling uiteengezette beginselen en met volledige inachtneming van het Handvest van de grondrechten, met name het daarin vastgelegde recht op vrijheid van meningsuiting en van informatie, en andere toepasselijke bepalingen van het Unierecht, in het bijzonder wat betreft de bescherming van persoonsgegevens, mededinging en elektronische handel.

2. De vooruitgang die in het kader van vrijwillige overeenkomsten tussen aanbieders van hostingdiensten en andere betrokken dienstverleners is bereikt met betrekking tot verschillende soorten illegale inhoud, wordt in deze aanbeveling verder uitgewerkt en geconsolideerd. Wat terroristische inhoud betreft, zorgt deze aanbeveling voor verdere uitwerking en consolidatie van de vooruitgang die in het kader van het EU-internetforum is geboekt.

3. Deze aanbeveling doet geen afbreuk aan de rechten en verplichtingen van de lidstaten om overeenkomstig het Unierecht maatregelen te nemen ten aanzien van illegale online-inhoud, met inbegrip van de mogelijkheid dat de rechterlijke en bestuurlijke autoriteiten van de lidstaten, overeenkomstig hun rechtsstelsel, aanbieders van hostingdiensten verplichten om illegale inhoud te verwijderen of ontoegankelijk te maken. Deze aanbeveling doet evenmin afbreuk aan de positie van aanbieders van hostingdiensten overeenkomstig Richtlijn 2000/31/EG en hun mogelijkheid om overeenkomstig het Unierecht en het recht van de lidstaten hun contractvoorwaarden vast te stellen en te handhaven.

([1]) Richtlijn (EU) 2016/680 van het Europees Parlement en de Raad van 27 april 2016 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens door bevoegde autoriteiten met het oog op de voorkoming, het onderzoek, de opsporing en de vervolging van strafbare feiten of de tenuitvoerlegging van straffen, en betreffende het vrije verkeer van die gegevens en tot intrekking van Kaderbesluit 2008/977/JBZ van de Raad (PB L 119 van 4.5.2016, blz. 89).

4. In het kader van deze aanbeveling wordt verstaan onder:

a) „aanbieder van hostingdiensten": een aanbieder van diensten van de informatiemaatschappij die bestaan in de opslag, op verzoek van een afnemer van de dienst, van door die afnemer verstrekte informatie, zoals bedoeld in artikel 14 van Richtlijn 2000/31/EG, ongeacht de plaats van vestiging van de aanbieder die zijn activiteiten richt op consumenten die in de Unie wonen;

b) „illegale inhoud": informatie die in strijd is met het recht van de Unie of het recht van de betrokken lidstaat;

c) „gebruiker": een natuurlijke persoon of rechtspersoon die de afnemer is van de dienst die wordt geleverd door een aanbieder van hostingdiensten;

d) „aanbieder van inhoud": een gebruiker die informatie heeft ingediend die op zijn verzoek wordt of is opgeslagen door een aanbieder van hostingdiensten;

e) „melding": een mededeling van een melder aan een aanbieder van hostingdiensten met betrekking tot door die aanbieder van hostingdiensten opgeslagen inhoud die de melder illegaal acht, waarbij de melder de aanbieder van hostingdiensten verzoekt om die inhoud op vrijwillige basis te verwijderen of ontoegankelijk te maken;

f) „melder": een natuurlijke persoon of een entiteit die een melding heeft ingediend bij een aanbieder van hostingdiensten;

g) „betrouwbare flagger": een natuurlijke persoon of een entiteit die volgens een aanbieder van hostingdiensten over bijzondere deskundigheid en verantwoordelijkheden beschikt voor de bestrijding van illegale online-inhoud;

h) „terroristische inhoud": informatie waarvan de verspreiding een terroristisch misdrijf vormt als bedoeld in Richtlijn (EU) 2017/541 of in de wetgeving van de betrokken lidstaat, met inbegrip van de verspreiding van relevante informatie die geproduceerd is door of kan worden toegeschreven aan een terroristische groepering of entiteit die is opgenomen in de desbetreffende lijsten die zijn opgesteld door de Unie of door de Verenigde Naties;

i) „rechtshandhavingsautoriteiten": de door de lidstaten overeenkomstig hun nationale recht aangewezen autoriteiten die bevoegd zijn voor het uitvoeren van rechtshandhavingstaken met het oog op het voorkomen, onderzoeken, opsporen of vervolgen van strafbare feiten in verband met illegale online-inhoud;

j) „bevoegde autoriteiten": de door de lidstaten overeenkomstig hun nationale recht aangewezen autoriteiten die bevoegd zijn voor het uitvoeren van taken die de bestrijding van illegale online-inhoud omvatten, met inbegrip van rechtshandhavingsautoriteiten en bestuurlijke autoriteiten die belast zijn met de handhaving van het recht dat van toepassing is op bepaalde specifieke gebieden, ongeacht de aard of het specifieke voorwerp van dat recht;

k) „doorverwijzing": een mededeling van een bevoegde autoriteit of van Europol aan een aanbieder van hostingdiensten met betrekking tot door die aanbieder van hostingdiensten opgeslagen inhoud die de bevoegde autoriteit of Europol als terroristische inhoud beschouwt, waarbij de bevoegde autoriteit of Europol de aanbieder van hostingdiensten verzoekt om die inhoud op vrijwillige basis te verwijderen of ontoegankelijk te maken.

HOOFDSTUK II

Algemene aanbevelingen met betrekking tot alle soorten illegale inhoud

Indiening en behandeling van meldingen

5. Er dient te worden voorzien in mechanismen voor het indienen van meldingen. Die mechanismen moeten gemakkelijk toegankelijk en gebruikersvriendelijk zijn en indiening met elektronische middelen mogelijk maken.

6. De mechanismen moeten het mogelijk maken en aanmoedigen dat voldoende nauwkeurige en goed onderbouwde meldingen worden ingediend, zodat de aanbieder van hostingdiensten een gemotiveerd en zorgvuldig besluit kan nemen ten aanzien van de inhoud waarop de melding betrekking heeft, met name over de vraag of de inhoud al dan niet illegaal moet worden geacht en of deze moet worden verwijderd of ontoegankelijk moet worden gemaakt. De mechanismen moeten zodanig van aard zijn dat zij het gemakkelijk maken meldingen te doen waarin de redenen waarom de melder de betrokken inhoud illegaal acht, worden uiteengezet en de plaats waar de inhoud is aangetroffen, duidelijk wordt aangegeven.

7. Melders moeten de mogelijkheid hebben, maar niet de plicht, om hun contactgegevens in de melding op te nemen. Besluiten zij hun contactgegevens te vermelden, dan moet hun anonimiteit jegens de aanbieder van inhoud worden gegarandeerd.

8. Indien de contactgegevens van de melder bekend zijn bij de aanbieder van hostingdiensten, moet deze de ontvangst van de melding bevestigen aan de melder en de melder onverwijld op evenredige wijze inlichten over zijn besluit met betrekking tot de inhoud die het onderwerp is van de melding.

Informatie aan aanbieders van inhoud en tegenmeldingen

9. Besluit een aanbieder van hostingdiensten om bij hem opgeslagen inhoud te verwijderen of ontoegankelijk te maken omdat hij de inhoud illegaal acht, ongeacht de wijze waarop de inhoud is opgespoord, geïdentificeerd, verwijderd of ontoegankelijk is gemaakt, en zijn de contactgegevens van de aanbieder van de inhoud bekend bij de aanbieder van hostingdiensten, dan dient de aanbieder van inhoud onverwijld en op evenredige wijze over dat besluit en de redenen daarvoor te worden ingelicht, alsook over de mogelijkheid om het besluit aan te vechten als bedoeld in punt 11.

10. Punt 9 dient echter niet van toepassing te zijn wanneer de betrokken inhoud duidelijk illegaal is en samenhangt met ernstige strafbare feiten die een bedreiging voor het leven of de veiligheid van personen inhouden. Daarnaast dienen aanbieders van hostingdiensten de in punt 9 bedoelde informatie niet te verstrekken, indien een bevoegde autoriteit daarom verzoekt om redenen van openbare orde en openbare veiligheid, en in het bijzonder met het oog op het voorkomen, onderzoeken, opsporen en vervolgen van strafbare feiten, zolang die autoriteit dat nodig acht.

11. Aanbieders van inhoud moeten de mogelijkheid krijgen om het in punt 9 bedoelde besluit van de aanbieder van hostingdiensten binnen een redelijke termijn aan te vechten door bij de aanbieder van hostingdiensten een tegenmelding in te dienen. Het mechanisme voor het indienen van tegenmeldingen moet gebruikersvriendelijk zijn en indiening met elektronische middelen mogelijk maken.

12. Er moet op worden toegezien dat aanbieders van hostingdiensten aan de door hen ontvangen tegenmeldingen passend gevolg geven. Indien de tegenmelding argumenten bevat die voor de aanbieder van hostingdiensten aanleiding zijn om aan te nemen dat de inhoud waarop de tegenmelding betrekking heeft, niet als illegaal moet worden beschouwd, moet hij zijn besluit om de inhoud te verwijderen of ontoegankelijk te maken, onverwijld herroepen, onverminderd zijn bevoegdheid om contractvoorwaarden vast te stellen en te handhaven overeenkomstig het Unierecht en het recht van de lidstaten.

13. De aanbieder van inhoud die een tegenmelding heeft ingediend, alsmede de betrokken melder, moeten — voor zover hun contactgegevens bekend zijn bij de betrokken aanbieder van hostingdiensten — onverwijld in kennis worden gesteld van het besluit dat de aanbieder van hostingdiensten heeft genomen ten aanzien van de betrokken inhoud.

Buitengerechtelijke geschillenbeslechting

14. De lidstaten worden aangemoedigd om, waar nuttig, buitengerechtelijke beslechting van geschillen met betrekking tot het verwijderen of ontoegankelijk maken van illegale inhoud te faciliteren. Dergelijke mechanismen voor buitengerechtelijke geschillenbeslechting moeten gemakkelijk toegankelijk, doeltreffend, transparant en onpartijdig zijn en ervoor zorgen dat eventuele schikkingen billijk zijn en in overeenstemming met het toepasselijke recht. Pogingen om tot een buitengerechtelijke beslechting van dergelijke geschillen te komen, mogen geen afbreuk doen aan het recht van de betrokken partijen om de zaak voor de rechter te brengen.

15. Wanneer de betrokken lidstaat daarin voorziet, worden aanbieders van hostingdiensten aangemoedigd om het gebruik van mechanismen voor buitengerechtelijke geschillenbeslechting toe te staan.

Transparantie

16. Aanbieders van hostingdiensten moeten worden aangemoedigd om duidelijke, begrijpelijke en voldoende gedetailleerde uitleg te geven van hun beleid ten aanzien van het verwijderen of ontoegankelijk maken van bij hen opgeslagen inhoud, met inbegrip van inhoud die illegaal wordt geacht.

17. Aanbieders van hostingdiensten moeten worden aangemoedigd om op gezette tijden, bij voorkeur ten minste eenmaal per jaar, verslag uit te brengen over hun activiteiten met betrekking tot het verwijderen en ontoegankelijk maken van inhoud die illegaal wordt geacht. In die verslagen dient met name informatie te worden opgenomen over de hoeveelheid inhoud die is verwijderd en de aard ervan, het aantal ontvangen meldingen en tegenmeldingen, en hoelang het duurde voor maatregelen werden genomen.

Proactieve maatregelen

18. Aanbieders van hostingdiensten moeten worden aangemoedigd om, waar mogelijk, evenredige en specifieke proactieve maatregelen te treffen ten aanzien van illegale inhoud. Die proactieve maatregelen kunnen onder meer betrekking hebben op het gebruik van geautomatiseerde middelen voor het opsporen van illegale inhoud, doch uitsluitend waar dat passend en evenredig is en er doeltreffende en passende waarborgen gelden, met name die bedoeld in de punten 19 en 20.

Waarborgen

19. Teneinde te voorkomen dat inhoud wordt verwijderd die niet illegaal is, moet worden voorzien in doeltreffende en passende waarborgen om ervoor te zorgen dat aanbieders van hostingdiensten zorgvuldig en evenredig optreden ten aanzien van inhoud die zij opslaan, met name bij het behandelen van meldingen en tegenmeldingen en bij het nemen van besluiten over het verwijderen of ontoegankelijk maken van inhoud die illegaal wordt geacht, zulks zonder dat afbreuk wordt gedaan aan de mogelijkheid voor aanbieders van hostingdiensten om hun contractvoorwaarden vast te stellen en te handhaven overeenkomstig het Unierecht en het recht van de lidstaten.

20. Wanneer aanbieders van hostingdiensten gebruikmaken van geautomatiseerde middelen ten aanzien van inhoud die zij opslaan, moet worden voorzien in doeltreffende en passende waarborgen om ervoor te zorgen dat besluiten met betrekking tot die inhoud, met name besluiten om inhoud die illegaal wordt geacht, te verwijderen of ontoegankelijk te maken, correct en gegrond zijn. Deze waarborgen moeten met name bestaan uit menselijk toezicht en menselijke verificatie, waar dat passend is, en in ieder geval wanneer een gedetailleerde beoordeling van de relevante context nodig is om vast te stellen of de inhoud illegaal moet worden geacht.

Bescherming tegen onrechtmatig gedrag

21. Er moeten doeltreffende en passende maatregelen worden getroffen om te voorkomen dat meldingen of tegenmeldingen worden gedaan die te kwader trouw zijn, of dat naar aanleiding van dergelijke meldingen of tegenmeldingen actie wordt ondernomen, alsook maatregelen tegen andere vormen van misbruik in verband met de maatregelen ter bestrijding van illegale online-inhoud waarin deze aanbeveling voorziet.

Samenwerking tussen aanbieders van hostingdiensten en lidstaten

22. Lidstaten en aanbieders van hostingdiensten moeten contactpunten aanwijzen voor aangelegenheden die verband houden met illegale online-inhoud.

23. Er moet worden voorzien in versnelde procedures voor de behandeling van meldingen van de bevoegde autoriteiten.

24. Met het oog op het voorkomen, onderzoeken, opsporen en vervolgen van strafbare feiten worden de lidstaten aangemoedigd om aanbieders van hostingdiensten er wettelijk toe te verplichten dat zij de rechtshandhavingsautoriteiten onverwijld inlichten over alle aanwijzingen voor mogelijke ernstige strafbare feiten die zij in het kader van hun activiteiten op het gebied van het verwijderen of ontoegankelijk maken van illegale inhoud hebben aangetroffen en die een bedreiging voor het leven of de veiligheid van personen vormen, zulks met inachtneming van de toepasselijke wettelijke vereisten, met name met betrekking tot de bescherming van persoonsgegevens, waaronder die van Verordening (EU) 2016/679.

Samenwerking tussen aanbieders van hostingdiensten en betrouwbare flaggers

25. De samenwerking tussen aanbieders van hostingdiensten en betrouwbare flaggers moet worden aangemoedigd. Er moet worden voorzien in versnelde procedures voor de behandeling van meldingen van betrouwbare flaggers.

26. Aanbieders van hostingdiensten moeten worden aangemoedigd om duidelijke en objectieve voorwaarden bekend te maken aan de hand waarvan zij bepalen welke personen of entiteiten zij als vertrouwde flaggers beschouwen.

27. Die voorwaarden moeten garanderen dat de betrokken personen of entiteiten beschikken over de nodige deskundigheid en hun activiteiten als betrouwbare flaggers uitvoeren op zorgvuldige en objectieve wijze, op basis van eerbiediging van de waarden waarop de Unie is gegrondvest.

Samenwerking tussen aanbieders van hostingdiensten

28. Aanbieders van hostingdiensten moeten, waar dat gepast is, ervaringen uitwisselen en technologische oplossingen en beste praktijken voor de bestrijding van illegale online-inhoud delen met elkaar en vooral met aanbieders van hostingdiensten die door hun omvang of de schaal waarop zij opereren, over beperkte middelen en deskundigheid beschikken. Dat moet onder meer gebeuren in het kader van de lopende samenwerking tussen aanbieders van hostingdiensten door middel van gedragscodes, memoranda van overeenstemming en andere vrijwillige regelingen.

HOOFDSTUK III

Specifieke aanbevelingen met betrekking tot terroristische inhoud

Algemeen

29. De specifieke aanbevelingen met betrekking tot terroristische inhoud in dit hoofdstuk zijn van toepassing in aanvulling op de algemene aanbevelingen in hoofdstuk II.

30. Aanbieders van hostingdiensten moeten in hun contractvoorwaarden uitdrukkelijk bepalen dat zij geen terroristische inhoud opslaan.

31. Aanbieders van hostingdiensten moeten maatregelen nemen om te voorkomen dat terroristische inhoud wordt opgeslagen, met name in verband met de doorverwijzingen, proactieve maatregelen en samenwerking bedoeld in de punten 32 tot en met 40.

Indiening en behandeling van doorverwijzingen

32. De lidstaten moeten erop toezien dat hun bevoegde autoriteiten in staat zijn en over voldoende middelen beschikken om terroristische inhoud op doeltreffende wijze op te sporen en doorverwijzingen in te dienen bij de betrokken aanbieders van hostingdiensten, met name via nationale eenheden voor de melding van internetuitingen en in samenwerking met de EU-eenheid voor de melding van internetuitingen bij Europol.

33. Er moet worden voorzien in mechanismen voor het indienen van doorverwijzingen. Voor het behandelen van doorverwijzingen moeten versnelde procedures worden opgezet, met name voor doorverwijzingen van de nationale eenheden voor de melding van internetuitingen en de EU-eenheid voor de melding van internetuitingen bij Europol.

34. Aanbieders van hostingdiensten moeten de ontvangst van doorverwijzingen onverwijld bevestigen en de bevoegde autoriteit of Europol inlichten over hun besluit met betrekking tot de doorverwezen inhoud, en in voorkomend geval aangeven of de inhoud is verwijderd of ontoegankelijk gemaakt, dan wel waarom is besloten de inhoud niet te verwijderen of ontoegankelijk te maken.

35. Aanbieders van hostingdiensten moeten in de regel uiterlijk één uur na de ontvangst van een doorverwijzing de betrokken inhoud beoordelen en zo nodig verwijderen of ontoegankelijk maken.

Proactieve maatregelen

36. Aanbieders van hostingdiensten moeten evenredige en specifieke proactieve maatregelen treffen, ook met gebruikmaking van geautomatiseerde middelen, om terroristische inhoud snel op te sporen, te identificeren en te verwijderen of ontoegankelijk te maken.

37. Aanbieders van hostingdiensten moeten evenredige en specifieke proactieve maatregelen treffen, ook met gebruikmaking van geautomatiseerde middelen, om onmiddellijk te voorkomen dat inhoud die al is verwijderd of ontoegankelijk is gemaakt omdat deze als terroristische inhoud wordt beschouwd, door aanbieders van inhoud opnieuw wordt aangeboden.

Samenwerking

38. Om te voorkomen dat terroristische inhoud wordt verspreid via verschillende hostingdiensten, moeten aanbieders van hostingdiensten worden aangemoedigd om samen te werken door effectieve, passende en proportionele technologische instrumenten te delen en te optimaliseren, met inbegrip van instrumenten waarmee inhoud geautomatiseerd kan worden opgespoord. Wanneer dat technologisch mogelijk is, moeten alle relevante vormen waarin terroristische inhoud wordt verspreid, worden opgespoord. Bij deze samenwerking moeten in het bijzonder aanbieders van hostingdiensten worden betrokken die door hun omvang of de schaal waarop zij opereren, over beperkte middelen en deskundigheid beschikken.

39. Aanbieders van hostingdiensten moeten worden aangemoedigd de maatregelen te nemen die nodig zijn voor de goede werking en de verbetering van de in punt 38 bedoelde instrumenten, in het bijzonder door identificatoren te verstrekken van alle als terroristisch beschouwde inhoud en door de mogelijkheden van deze instrumenten volledig te benutten.

40. De bevoegde autoriteiten en aanbieders van hostingdiensten moeten werkafspraken maken, waar mogelijk ook met Europol, over aangelegenheden in verband met terroristische online-inhoud, die erop gericht moeten zijn het inzicht in terroristische onlineactiviteiten te vergroten, de doorverwijzingsmechanismen te verbeteren, onnodig dubbel werk te voorkomen en verzoeken van rechtshandhavingsautoriteiten met het oog op strafrechtelijk onderzoek in verband met terrorisme te vergemakkelijken.

HOOFDSTUK IV

Informatieverstrekking

41. De lidstaten moeten op gezette tijden, bij voorkeur om de drie maanden, verslag uitbrengen aan de Commissie over de doorverwijzingen die hun bevoegde autoriteiten hebben ingediend, en de besluiten die aanbieders van hostingdiensten naar aanleiding daarvan hebben genomen, alsmede over hun samenwerking met aanbieders van hostingdiensten met betrekking tot de bestrijding van terroristische inhoud.

42. Om mogelijk te maken dat het aan deze aanbeveling gegeven gevolg met betrekking tot terroristische inhoud uiterlijk drie maanden na de bekendmaking van deze aanbeveling wordt gemonitord, dienen de aanbieders van hostingdiensten op verzoek van de Commissie haar alle informatie te verstrekken die voor de monitoring vereist is. Daarbij kan het met name gaan om informatie over de hoeveelheid inhoud die is verwijderd of ontoegankelijk is gemaakt, hetzij naar aanleiding van meldingen of doorverwijzingen, hetzij door middel van proactieve maatregelen en het gebruik van geautomatiseerde middelen. Ook het aantal ontvangen verwijzingen en de tijd die nodig was voor het nemen van maatregelen, alsmede de hoeveelheid inhoud waarvan de aanbieding of hernieuwde aanbieding door toepassing van geautomatiseerde opsporing en andere technologische instrumenten is verhinderd, kunnen worden vermeld.

43. Om mogelijk te maken dat het aan deze aanbeveling gegeven gevolg met betrekking tot andere illegale inhoud dan terroristische inhoud uiterlijk zes maanden na de bekendmaking ervan wordt gemonitord, dienen de lidstaten en de aanbieders van hostingdiensten op verzoek van de Commissie haar alle informatie te verstrekken die voor de monitoring vereist is.

Gedaan te Brussel, 1 maart 2018.

Voor de Commissie
Andrus ANSIP
Vicevoorzitter