# REKOMMENDATIONER

## KOMMISSIONENS REKOMMENDATION (EU) 2018/334

## av den 1 mars 2018

## om åtgärder för att effektivt bekämpa olagligt innehåll online

EUROPEISKA KOMMISSIONEN HAR ANTAGIT DENNA REKOMMENDATION

med beaktande av fördraget om Europeiska unionens funktionssätt, särskilt artikel 292, och

av följande skäl:

(1) Internet och tjänsteleverantörer som är verksamma på nätet bidrar i hög grad till innovation, ekonomisk tillväxt och jobbskapande i unionen. Många av dessa tjänsteleverantörer spelar en avgörande roll i den digitala ekonomin genom att de för samman företag och privatpersoner, främjar den offentliga debatten och gör det lättare att sprida och ta emot fakta, åsikter och idéer. Tjänsterna missbrukas emellertid i vissa fall av tredje parter för att bedriva olaglig verksamhet online, till exempel sprida information som rör terrorism, sexuellt utnyttjande av barn, olaglig hatpropaganda eller brott mot konsumentskyddslagar, vilket kan undergräva användarnas förtroende för dem och skada deras affärsmodell. Ibland kan de berörda tjänsteleverantörerna till och med dra viss nytta av sådan verksamhet, till exempel som en följd av att upphovsrättsligt skyddat innehåll är tillgängligt utan rättsinnehavarnas tillstånd.

(2) Förekomsten av olagligt innehåll online har allvarliga negativa konsekvenser för användare, för andra berörda personer och företag samt för samhället i stort. Leverantörer av onlinetjänster har, på grund av sin centrala roll och de tekniska hjälpmedel och den tekniska kapacitet som förknippas med tjänsterna, ett särskilt samhällsansvar när det gäller att komma till rätta med olagligt innehåll som sprids med hjälp av deras tjänster.

(3) Med tanke på att det ofta är av avgörande betydelse att olagligt innehåll snabbt avlägsnas eller blockeras för att begränsa vidare spridning och skada innebär detta ansvar bland annat att de berörda tjänsteleverantörerna bör kunna fatta snabba beslut om möjliga åtgärder mot olagligt innehåll på nätet. Detta ansvar innebär också att de bör införa effektiva och lämpliga skyddsåtgärder, framför allt för att se till att de agerar på ett samvetsgrant och proportionerligt sätt och för att förhindra oavsiktligt avlägsnande av innehåll som inte är olagligt.

(4) Många leverantörer av onlinetjänster har vidkänts detta ansvar och följaktligen skridit till handling. På en kollektiv nivå har viktiga framsteg gjorts genom frivilliga arrangemang av olika slag, t.ex. EU:s internetforum om terrorisminnehåll online, uppförandekoden om att motverka olaglig hatpropaganda online och samförståndsavtalet om försäljning av varumärkesförfalskade varor. Trots dessa åtaganden och framsteg är olagligt innehåll på nätet fortfarande ett allvarligt problem i EU.

(5) Med anledning av en rad terroristattacker i EU och spridningen av terroristpropaganda på nätet uttryckte Europeiska rådet efter sitt möte den 22 och 23 juni 2017 sin oro och sade att det förväntar sig att sektorn ska ”utveckla nya tekniker och verktyg i syfte att förbättra den automatiska upptäckten av och raderingen av innehåll som uppviglar till terroristdåd”. I Europaparlamentets resolution av den 15 juni 2017 uppmanades dessa onlineplattformar enträget ”att vidta kraftigare åtgärder mot olagligt och skadligt innehåll”. Uppmaningen att företagen ska vara mer proaktiva i fråga om att skydda sina användare från terrorisminnehåll har upprepats av medlemsstaternas ministrar inom ramen för EU:s internetforum. I rådets slutsatser av den 4 december 2014 om säkerställande av skyddet för immateriella rättigheter uppmanades kommissionen att överväga att använda tillgängliga verktyg för att identifiera personer som gör immaterialrättsliga intrång och mellanhändernas roll till stöd för kampen mot immaterialrättsintrång.

(6) Den 28 september 2017 antog kommissionen ett meddelande med riktlinjer om det ansvar leverantörer av onlinetjänster har i fråga om olagligt innehåll online ([1]). I meddelandet uppgav kommissionen att den skulle bedöma om det behövs fler åtgärder, bland annat genom att övervaka framstegen på grundval av frivilliga arrangemang. Denna rekommendation följer upp meddelandet på samma ambitionsnivå och ger det verkan samtidigt som rekommendationen tar vederbörlig hänsyn till och bygger vidare på de viktiga framsteg som har gjorts genom dessa frivilliga arrangemang.

(7) I rekommendationen poängteras att vederbörlig hänsyn bör tas till de särskilda omständigheterna när det gäller hantering av olika typer av olagligt innehåll på nätet och de särskilda insatser som kan krävas, bland annat genom särskilda lagstiftningsåtgärder. Till exempel antog kommissionen den 25 maj 2016 som en bekräftelse på behovet av sådana särskilda lagstiftningsåtgärder ett förslag till ändring av Europaparlamentets och rådets direktiv 2010/13/EU ([2]), mot bakgrund av ändrade marknadsförhållanden. Den 14 september 2016 antog den också ett förslag till direktiv om upphovsrätt på den digitala inre marknaden ([3]) där det föreskrivs en skyldighet för vissa tjänsteleverantörer att i samarbete med rättsinnehavare vidta åtgärder för att säkerställa tillämpningen av avtal med rättsinnehavare för användning av deras verk eller andra alster eller för att hindra tillgång via deras tjänster till verk eller andra alster som identifierats av rättsinnehavare genom samarbete med tjänsteleverantörerna. Denna rekommendation påverkar inte dessa lagstiftningsåtgärder och förslag.

(8) Europaparlamentets och rådets direktiv 2000/31/EG ([4]) innehåller undantag från ansvar vilka, på vissa villkor, är tillgängliga för vissa leverantörer av onlinetjänster, bland annat leverantörer av ”värdtjänster” i den mening som avses i artikel 14 i direktivet. För att kunna utnyttja undantaget från ansvar ska värdtjänstleverantörer agera utan dröjsmål för att avlägsna den olagliga information de lagrar eller göra den oåtkomlig så snart de fått kännedom om den och, beträffande skadeståndsanspråk, blivit medvetna om fakta eller omständigheter som gjort förekomsten av den olagliga verksamheten eller den olagliga informationen uppenbar. De kan få den kännedomen och medvetenheten bland annat genom anmälningar. Som sådant utgör direktiv 2000/31/EG grunden för utvecklingen av förfaranden som syftar till att avlägsna och blockera olaglig information. Direktivet ger också medlemsstaterna möjlighet att kräva att de berörda tjänsteleverantörerna tillämpar en omsorgsplikt när det gäller olagligt innehåll som de kan lagra.

(9) När medlemsstaterna vidtar åtgärder mot olagligt innehåll på nätet ska de respektera den princip om ursprungsland som fastställs i direktiv 2000/31/EG. Enligt den får de inte av skäl som omfattas av det samordnade område som definieras i direktivet begränsa den fria rörligheten för informationssamhällets tjänster för tjänsteleverantörer som är etablerade i en annan medlemsstat, dock under förutsättning att det finns möjlighet till undantag på vissa villkor som anges i direktivet.

(10) Dessutom föreskrivs i flera andra unionsrättsakter en rättslig ram för vissa typer av olagligt innehåll som är tillgängligt och sprids på nätet. I synnerhet kräver Europaparlamentets och rådets direktiv 2011/93/EU ([5]) att medlemsstaterna vidtar åtgärder för att avlägsna webbsidor som innehåller eller sprider barnpornografi och åtgärder som ger dem möjlighet att blockera tillträdet till sådana sidor, med förbehåll för vissa skyddsåtgärder. Europaparlamentets och rådets direktiv (EU) 2017/541 ([6]), som ska ha införlivats i nationell lagstiftning senast den 8 september 2018, innehåller liknande bestämmelser om internetinnehåll som utgör offentlig uppmaning till terroristbrott. I direktiv (EU) 2017/541 anges även minimiregler om fastställande av brottsrekvisit på området terroristbrott, brott med anknytning till en terroristgrupp och brott med anknytning till terroristverksamhet.

([1]) COM(2017) 555 final av den 28 september 2017.
([2]) Europaparlamentets och rådets direktiv 2010/13/EU av den 10 mars 2010 om samordning av vissa bestämmelser som fastställs i medlemsstaternas lagar och andra författningar om tillhandahållande av audiovisuella medietjänster (direktiv om audiovisuella medietjänster) (EUT L 95, 15.4.2010, s. 1). COM(2016) 287 final.
([3]) COM(2016) 593 final av den 14 september 2016.
([4]) Europaparlamentets och rådets direktiv 2000/31/EG av den 8 juni 2000 om vissa rättsliga aspekter på informationssamhällets tjänster, särskilt elektronisk handel, på den inre marknaden (”direktiv om elektronisk handel”) (EGT L 178, 17.7.2000, s. 1).
([5]) Europaparlamentets och rådets direktiv 2011/93/EU av den 13 december 2011 om bekämpande av sexuella övergrepp mot barn, sexuell exploatering av barn och barnpornografi samt om ersättande av rådets rambeslut 2004/68/RIF (EUT L 335, 17.12.2011, s. 1).
([6]) Europaparlamentets och rådets direktiv (EU) 2017/541 av den 15 mars 2017 om bekämpande av terrorism, om ersättande av rådets rambeslut 2002/475/RIF och om ändring av rådets beslut 2005/671/RIF (EUT L 88, 31.3.2017, s. 6).

Enligt Europaparlamentets och rådets direktiv 2004/48/EG ([1]) är det möjligt för behöriga rättsliga myndigheter att utfärda förelägganden mot mellanhänder vars tjänster utnyttjas av tredje man för att göra immaterialrättsintrång.

(11) I synnerhet mot denna bakgrund har några medlemsstater, utöver de frivilliga åtgärder som vidtagits av vissa leverantörer av onlinetjänster, antagit regler om mekanismer för anmälan och åtgärd sedan antagandet av direktiv 2000/31/EG. Andra medlemsstater överväger att införa sådana regler. Dessa mekanismer syftar i allmänhet till att underlätta anmälning av innehåll som den anmälande parten anser vara olagligt till den berörda värdtjänstleverantören (anmälan), varpå leverantören kan besluta om huruvida den håller med om bedömningen och önskar avlägsna eller blockera innehållet (åtgärd). Skillnaderna mellan de nationella reglerna blir allt större. På grund av detta kan de berörda tjänsteleverantörerna bli föremål för en rad rättsliga krav som skiljer sig åt till både innehåll och omfattning.

(12) I den inre marknadens intresse samt för att effektivisera kampen mot olagligt innehåll på nätet och skydda den balanserade strategi som direktiv 2000/31/EG syftar till att säkerställa är det nödvändigt att fastställa vissa huvudprinciper som bör vara vägledande för medlemsstaternas och de berörda tjänsteleverantörernas åtgärder i detta avseende.

(13) Dessa principer bör fastställas och tillämpas med full respekt för de grundläggande rättigheter som skyddas i unionens rättsordning, framför allt de som garanteras i Europeiska unionens stadga om de grundläggande rättigheterna (nedan kallad *stadgan*). Olagligt innehåll på nätet bör hanteras med lämpliga och verkningsfulla skyddsåtgärder för att säkerställa skyddet av de olika grundläggande rättigheter som står på spel för alla berörda parter. Rättigheterna kan till exempel vara yttrandefriheten (även friheten att ta emot och sprida uppgifter), rätten till respekt för privatlivet och skydd av personuppgifter samt rätten till ett effektivt domstolsskydd för användarna av tjänsterna i fråga. De kan också vara näringsfrihet, inklusive avtalsfrihet, för värdtjänstleverantören samt barnets rättigheter och rätten till skydd av egendom, inklusive immateriell egendom, till människans värdighet och till icke-diskriminering av vissa andra berörda parter. I synnerhet bör värdtjänstleverantörer, när de fattar beslut om att avlägsna eller blockera innehåll som de lagrar, ta vederbörlig hänsyn till användarnas grundläggande rättigheter och berättigade intressen samt den centrala roll som dessa leverantörer tenderar att spela i underlättandet av den offentliga debatten och spridningen och mottagandet av fakta, åsikter och idéer i enlighet med lagen.

(14) I enlighet med det övergripande arbetssätt som ligger till grund för det undantag från ansvar som anges i artikel 14 i direktiv 2000/31/EG bör denna rekommendation tillämpas på alla typer av innehåll som inte stämmer överens med unionslagstiftningen eller medlemsstaternas lagstiftning, oavsett lagstiftningens exakta sakinnehåll eller karaktär. Det är tillräckligt att ta hänsyn till lagarna i de medlemsstater som berörs av de aktuella tjänsterna, främst den medlemsstat där leverantören är etablerad och den där tjänsten erbjuds. Dessutom bör det vid tillämpningen av denna rekommendation tas vederbörlig hänsyn till hur allvarligt det olagliga innehållet är och vilken potentiell skada som uppstått på grund av det, vilket kan vara nära kopplat till hur snabbt åtgärder vidtas och till vad som rimligen kan förväntas av värdtjänstleverantörerna, i tillämpliga fall med tanke på utvecklingen och möjlig användning av teknik. Vederbörlig hänsyn bör även tas till de relevanta skillnader som kan finnas mellan olika typer av olagligt innehåll och vilka åtgärder som ska vidtas för att ta itu med dem.

(15) Värdtjänstleverantörer spelar en särskilt viktig roll i arbetet mot olagligt innehåll online, eftersom de lagrar information som tillhandahålls av deras användare på användarnas begäran och ger andra användare tillgång till den, ofta i stor skala. Denna rekommendation avser därför huvudsakligen dessa leverantörers verksamhet och skyldigheter. Rekommendationerna kan dock också i tillämpliga delar gälla andra berörda leverantörer av onlinetjänster. Eftersom syftet med denna rekommendation är att hantera de risker som är förknippade med olagligt innehåll online och som påverkar konsumenter i EU rör den samtliga värdtjänstleverantörers verksamhet, oavsett om de är etablerade i unionen eller i ett tredjeland, förutsatt att de riktar sin verksamhet till konsumenter som bor i unionen.

(16) Mekanismer för att anmäla innehåll som anses vara olagligt innehåll till värdtjänstleverantörer är viktiga för att bekämpa olagligt innehåll på nätet. Sådana mekanismer bör göra det lättare för alla personer eller enheter som

([1]) Europaparlamentets och rådets direktiv 2004/48/EG av den 29 april 2004 om säkerställande av skyddet för immateriella rättigheter (EUT L 157, 30.4.2004, s. 45).

vill göra en anmälan. Därför bör dessa mekanismer vara lätta att tillgå och använda för alla användare. Värdtjänstleverantörer bör dock förbli flexibla, till exempel när det gäller rapporteringsformat eller teknik som ska användas, för att möjliggöra effektiva lösningar och undvika orimliga bördor för dessa leverantörer.

(17) I enlighet med rättspraxis från Europeiska unionens domstol avseende artikel 14 i direktiv 2000/31/EG bör anmälningarna vara tillräckligt precisa och underbyggda för att den värdtjänstleverantör som tar emot dem ska kunna fatta ett välgrundat och omsorgsfullt beslut om hur anmälan ska följas upp. Det bör därför i så stor utsträckning som möjligt säkerställas att den standarden uppfylls. Men huruvida en viss anmälan leder till kännedom eller medvetenhet i den mening som avses i artikel 14 i direktivet ska bedömas mot bakgrund av omständigheterna i ärendet i fråga, med beaktande av att sådan kännedom eller medvetenhet också kan fås på annat sätt än genom anmälningar.

(18) Värdtjänstleverantören måste i allmänhet inte ha anmälarens kontaktuppgifter för att kunna fatta ett välgrundat och omsorgsfullt beslut om uppföljning av anmälningen. Det skulle innebära ett hinder för anmälan om man gjorde det obligatoriskt att tillhandahålla kontaktuppgifter vid inlämnandet. Kontaktuppgifter är dock nödvändiga för att värdtjänstleverantören ska kunna ge återkoppling. Anmälaren bör därför ha en valfri möjlighet att lämna sina kontaktuppgifter.

(19) För att öka öppenheten och exaktheten hos mekanismen för anmälan och åtgärd och för att möjliggöra prövning vid behov bör värdtjänstleverantörer, om de har anmälarens och/eller innehållsleverantörens kontaktuppgifter, inom rimlig tid och på lämpligt sätt informera dessa personer om vilka steg som har tagits i samband med nämnda mekanismer, i synnerhet när det gäller beslut om att avlägsna eller blockera det berörda innehållet i enlighet med anmälan. Den information som ska ges bör vara proportionerlig, dvs. den bör motsvara de uppgifter som de berörda personerna har lämnat i sin anmälan eller motanmälan, och samtidigt möjliggöra lämpliga och differentierade lösningar utan att leda till en alltför stor börda för leverantörerna.

(20) För att sörja för öppenhet och rättvisa och undvika oavsiktligt avlägsnande av innehåll som inte är olagligt innehåll bör innehållsleverantörer i princip informeras om beslutet att avlägsna eller blockera det innehåll som lagras på deras begäran och ges möjlighet att bestrida beslutet genom en motanmälan, i syfte att i tillämpliga fall få beslutet upphävt, oavsett om det fattades till följd av en anmälan, ett hänskjutande eller proaktiva åtgärder från värdtjänstleverantörens sida.

(21) Med tanke på det aktuella innehållets karaktär, syftet med ett sådant motanmälningsförfarande och den ytterligare börda som det innebär för värdtjänstleverantörer finns det dock ingen grund för att rekommendera att information ges om beslutet och möjligheten att bestrida det när det är uppenbart att innehållet i fråga är olagligt innehåll och rör allvarliga brott som innebär ett hot mot människors liv eller säkerhet, såsom de brott som anges i direktiven (EU) 2017/541 och 2011/93/EU. Dessutom kan det i vissa fall av hänsyn till allmän ordning och säkerhet, i synnerhet för att förebygga, utreda, upptäcka och lagföra brott, vara motiverat att inte direkt ge denna information till den berörda innehållsleverantören. Därför bör värdtjänstleverantörer låta bli att göra det om en behörig myndighet begär detta av hänsyn till allmän ordning och säkerhet, under så lång tid som myndigheten har begärt detta mot bakgrund av dessa hänsyn. I den mån detta innebär en begränsning av rätten att bli informerad om behandling av personuppgifter ska de relevanta villkoren i Europaparlamentets och rådets förordning (EU) 2016/679 ([1]) iakttas.

(22) Mekanismer för anmälan och åtgärd bör inte på något sätt påverka parternas rätt att inleda rättsliga förfaranden, i enlighet med tillämplig lagstiftning, avseende något innehåll som anses vara olagligt innehåll eller några åtgärder som vidtas av värdtjänstleverantörerna i detta avseende. Mekanismer för lösning utanför domstol av tvister som uppkommer i detta sammanhang kan vara ett viktigt komplement till rättsliga förfaranden, i synnerhet när de möjliggör effektiv, ekonomiskt överkomlig och snabb lösning av sådana tvister. Tvistlösning utanför domstol bör därför uppmuntras, förutsatt att de relevanta mekanismerna uppfyller vissa standarder, främst i fråga om rättvisa förfaranden, att parternas tillgång till domstolsprövning inte påverkas och att missbruk undviks.

([1]) Europaparlamentets och rådets förordning (EU) 2016/679 av den 27 april 2016 om om skydd för fysiska personer med avseende på behandling av personuppgifter och om det fria flödet av sådana uppgifter och om upphävande av direktiv 95/46/EG (allmän dataskyddsförordning) (EUT L 119, 4.5.2016, s. 1).

(23) För att bättre kunna bedöma effektiviteten hos mekanismerna för anmälan och åtgärd och värdtjänstleverantörernas andra åtgärder avseende innehåll som anses vara olagligt innehåll och för att sörja för ansvarsskyldighet bör det råda öppenhet gentemot allmänheten. Värdtjänstleverantörer bör därför regelbundet offentliggöra rapporter om dessa mekanismer och annan verksamhet, vilka bör vara tillräckligt fullständiga och detaljerade för att möjliggöra en tillräcklig insyn. De bör också i sina användarvillkor sörja för tydlighet i förväg om sin policy om att avlägsna eller blockera innehåll som de lagrar, däribland olagligt innehåll.

(24) Utöver mekanismerna för anmälan och åtgärd kan proportionella och specifika proaktiva åtgärder som vidtas frivilligt av värdtjänstleverantörer, även med hjälp av automatiska verktyg i vissa fall, också vara en viktig faktor för att komma till rätta med olagligt innehåll på nätet, utan att det påverkar tillämpningen av artikel 15.1 i direktiv 2000/31/EG. I samband med sådana proaktiva åtgärder bör hänsyn tas till situationen för värdtjänstleverantörer som på grund av sin storlek eller verksamhetens omfattning endast har begränsade resurser och sakkunskaper, och till behovet av effektiva och lämpliga skyddsåtgärder i samband med sådana åtgärder.

(25) Det kan i synnerhet vara lämpligt att vidta sådana proaktiva åtgärder när det redan har fastställts att innehållet är olagligt innehåll eller om innehållet är av en sådan typ att sammanhanget inte är viktigt. Det kan också bero på de planerade åtgärdernas art, omfattning och syfte och det berörda innehållets typ, på om innehållet har anmälts av brottsbekämpande myndigheter eller Europol samt på om åtgärder redan har vidtagits avseende innehållet eftersom det anses vara olagligt innehåll. I synnerhet när det gäller barnpornografi bör värdtjänstleverantörer vidta proaktiva åtgärder för att upptäcka och förhindra spridningen av sådant material, i enlighet med de åtaganden som gjorts inom ramen för den globala alliansen mot sexuell exploatering av barn på internet.

(26) I detta sammanhang har kommissionen i sitt meddelande av den 28 september 2017 om hantering av olagligt innehåll online fört fram sin åsikt att sådana frivilliga, proaktiva åtgärder inte automatiskt leder till att värdtjänstleverantören i fråga förlorar fördelen med det undantag från ansvar som föreskrivs i artikel 14 i direktiv 2000/31/EG.

(27) Det är mycket viktigt att alla åtgärder för att bekämpa olagligt innehåll på nätet omfattas av effektiva och lämpliga skyddsåtgärder som syftar till att se till att värdtjänstleverantörer agerar på ett samvetsgrant och proportionerligt sätt när de fastställer och genomdriver sin policy i fråga om innehåll som de lagrar, även olagligt innehåll, så att det i synnerhet garanteras att användarna fritt kan ta emot och sprida information online i enlighet med tillämplig lagstiftning. Utöver eventuella skyddsåtgärder som föreskrivs i den tillämpliga lagstiftningen, t.ex. om skyddet av personuppgifter, bör särskilda skyddsåtgärder, framför allt mänsklig övervakning och kontroll, föreskrivas och tillämpas när det är lämpligt vid användning av automatiska verktyg, för att undvika oavsiktliga och felaktiga beslut.

(28) Smidigt, effektivt och lämpligt samarbete mellan behöriga myndigheter och värdtjänstleverantörer bör säkerställas vid bekämpning av olagligt innehåll på nätet. Samarbetet kan i förekommande fall gagnas av Europols bistånd, till exempel vid bekämpning av terrorism, sexuella övergrepp och sexuell exploatering av barn, barnpornografi och kontaktsökning med barn i sexuellt syfte. För att underlätta detta samarbete bör medlemsstaterna och värdtjänstleverantörer utse kontaktpunkter, och förfaranden bör inrättas för behandling av dessa myndigheters anmälningar som en prioriterad fråga och med en lämplig grad av tillförlitlighet vad gäller deras korrekthet, med beaktande av myndigheternas särskilda sakkunskap och ansvar. För att effektivt komma till rätta med vissa särskilt allvarliga brott, som de brott som anges i direktiven (EU) 2017/541 och 2011/93/EU, som värdtjänstleverantörer kan komma att upptäcka när de bedriver sin verksamhet, bör medlemsstaterna uppmuntras att använda sig av den möjlighet som föreskrivs i artikel 15.2 i direktiv 2000/31/EG att lagstadga rapporteringskrav, i enlighet med tillämplig lagstiftning, framför allt förordning (EU) 2016/679.

(29) Förutom de behöriga myndigheterna kan vissa personer eller enheter, t.ex. icke-statliga organisationer och branschorganisationer, också ha särskild sakkunskap och på frivillig basis vilja ta sig an ett visst ansvar för bekämpning av olagligt innehåll på nätet. Med tanke på mervärdet och det ibland stora antalet anmälningar som berörs bör samarbete mellan sådana betrodda anmälare och värdtjänstleverantörer uppmuntras, i synnerhet genom att behandla även deras anmälningar med prioritet och med en lämplig grad av tillförlitlighet vad gäller deras korrekthet. Emellertid bör det samarbetet, i enlighet med de betrodda anmälarnas särskilda status, endast

vara öppet för personer och enheter som respekterar de värden som unionen bygger på enligt artikel 2 i fördraget om Europeiska unionen och som uppfyller vissa lämpliga tydliga, objektiva och offentliggjorda villkor.

(30) Bekämpning av olagligt innehåll på nätet kräver en helhetsstrategi, eftersom sådant innehåll ofta lätt flyttas från en värdtjänstleverantör till en annan, varvid de svagaste länkarna i kedjan utnyttjas. Samarbete är därför av avgörande betydelse, i synnerhet frivillig delning av erfarenheter, tekniska lösningar och bästa praxis. Sådant samarbete är särskilt viktigt när det gäller värdtjänstleverantörer som på grund av sin storlek eller verksamhetens omfattning endast har begränsade resurser och sakkunskaper.

(31) Terrorism innebär olaglig och urskillningslös användning av våld och hot mot andra människor. Terrorister förlitar sig allt mer på internet för att sprida terroristpropaganda och använder ofta sofistikerade metoder för snabb och bred spridning. Även om framsteg har gjorts i synnerhet inom EU:s internetforum finns det fortfarande ett trängande behov av snabbare och effektivare motåtgärder mot terrorisminnehåll på nätet, utöver behovet för de värdtjänstleverantörer som deltar i EU:s internetforum att fullt ut leva upp till sina åtaganden när det gäller effektiv och omfattande rapportering.

(32) Mot bakgrund av de särskilda omständigheterna i kampen mot terrorisminnehåll online bör rekommendationerna om hantering av olagligt innehåll i allmänhet kompletteras med vissa rekommendationer som specifikt rör bekämpning av terrorisminnehåll på nätet, genom att bygga vidare på och befästa de insatser som gjorts inom ramen för EU:s internetforum.

(33) Med tanke på de särskilt allvarliga risker som terrorisminnehåll medför och värdtjänstleverantörernas centrala roll i spridningen av sådant innehåll bör värdtjänstleverantörer vidta alla rimliga åtgärder för att inte tillåta terrorisminnehåll och om möjligt undvika att hysa det, med förbehåll för deras möjlighet att fastställa och genomdriva sina användarvillkor och behovet av effektiva och lämpliga skyddsåtgärder och utan att det påverkar tillämpningen av artikel 14 i direktiv 2000/31/EG.

(34) Dessa åtgärder bör framför allt bestå i samarbete med behöriga myndigheter och Europol i samband med hänskjutanden, som är en särskild metod för att göra anmälningar till värdtjänstleverantörer vilken är anpassad till de särskilda omständigheterna i kampen mot terrorisminnehåll. Vid hänskjutanden bör behöriga myndigheter och Europol kunna begära att innehåll som de anser vara terrorisminnehåll avlägsnas eller blockeras, antingen med hänvisning till tillämpliga lagar eller den berörda värdtjänstleverantörens användarvillkor. Dessa hänskjutandemekanismer bör finnas utöver de andra mekanismer för att anmäla innehåll (även för betrodda anmälare) som också kan användas för att anmäla innehåll som anses vara terrorisminnehåll.

(35) Med tanke på att terrorisminnehåll vanligen gör mest skada inom en timme efter att det först läggs ut på nätet, och med tanke på de behöriga myndigheternas och Europols särskilda sakkunskap och ansvar, bör hänskjutanden som en allmän regel bedömas och vid behov följas upp genom åtgärder inom en timme.

(36) Dessa insatser mot terrorisminnehåll bör också bestå av proportionella och särskilda proaktiva åtgärder, bl.a. med hjälp av automatiska verktyg, för att upptäcka, identifiera och snabbt avlägsna eller blockera terrorisminnehåll och för att se till att terrorisminnehåll inte dyker upp igen, utan att det påverkar tillämpningen av artikel 15.1 i direktiv 2000/31/EG. I detta avseende bör hänsyn tas till behovet av adekvata och effektiva skyddsåtgärder i samband med sådana åtgärder, i synnerhet de som rekommenderas i kapitel II i denna rekommendation.

(37) Samarbete, både värdtjänstleverantörer emellan och mellan dem och behöriga myndigheter, är av yttersta vikt i kampen mot terrorisminnehåll på nätet. I synnerhet kan tekniska verktyg som möjliggör automatisk upptäckt av innehåll, som databasen över hasher, bidra till att nå målet att förhindra spridning av terrorisminnehåll mellan olika värdtjänster. Sådant samarbete och utvecklingen, driften och utbytet av sådana tekniska verktyg bör uppmuntras, med hjälp av Europols expertis när så är lämpligt. Dessa gemensamma insatser är särskilt viktiga för att hjälpa värdtjänstleverantörer som har begränsade resurser och sakkunskaper, på grund av sin storlek eller verksamhetens omfattning, att kunna agera snabbt och effektivt på hänskjutanden och vidta proaktiva åtgärder enligt rekommendationen.

(38) Så många relevanta värdtjänstleverantörer som möjligt bör ansluta sig till dessa gemensamma insatser och alla deltagande värdtjänstleverantörer bör hjälpa till att optimera och maximera användningen av dessa verktyg. Ingåendet av samarbetsavtal mellan alla berörda parter, även Europol när det är lämpligt, bör också uppmuntras, med tanke på att sådana arrangemang kan bidra till en konsekvent och effektiv strategi och möjliggöra utbyte av relevanta erfarenheter och sakkunskaper.

(39) För att garantera respekten för den grundläggande rätten till skydd av fysiska personer med avseende på behandling av personuppgifter samt det fria flödet av personuppgifter, bör behandlingen av personuppgifter i samband med alla åtgärder som vidtas för att ge verkan åt denna rekommendation genomföras i full överensstämmelse med dataskyddsreglerna, i synnerhet förordning (EU) 2016/679 och Europaparlamentets och rådets direktiv (EU) 2016/680 ([1]), och behandlingen bör övervakas av de behöriga tillsynsmyndigheterna.

(40) Denna rekommendation är förenlig med de grundläggande rättigheter och de principer som erkänns särskilt i stadgan. I synnerhet syftar rekommendationen till att garantera full respekt för artiklarna 1, 7, 8, 10, 11, 16, 17, 21, 24 och 47 i stadgan.

(41) Kommissionen har för avsikt att noga övervaka alla åtgärder som vidtas till följd av denna rekommendation. Medlemsstaterna och värdtjänstleverantörer bör därför vara beredda att på kommissionens begäran tillställa den all relevant information som de rimligen kan förväntas tillhandahålla för att möjliggöra denna övervakning. På grundval av den information som inhämtats på detta sätt och all annan tillgänglig information, bland annat rapportering utifrån olika frivilliga arrangemang, kommer kommissionen att bedöma hur denna rekommendation har omsatts i praktiken och besluta om det krävs ytterligare steg, t.ex. förslag om bindande unionsrättsakter. Bekämpningen av terrorisminnehåll på nätet kräver särskilda och brådskande åtgärder, varför denna övervakning och utvärdering bör utföras på grundval av detaljerad information och särskilt snabbt – inom tre månader från och med dagen för offentliggörandet av denna rekommendation – medan det för andra typer av olagligt innehåll är lämpligt att göra detta sex månader efter offentliggörandet.

HÄRIGENOM REKOMMENDERAS FÖLJANDE.

## KAPITEL I

## Syfte och termer

1. Medlemsstaterna och värdtjänstleverantörer, när det gäller innehåll som de lagrar på begäran av innehållsleverantörer, uppmanas att vidta effektiva, lämpliga och proportionerliga åtgärder för att ta itu med olagligt innehåll online, i enlighet med de principer som anges i denna rekommendation och i full överensstämmelse med stadgan, framför allt rätten till yttrande- och informationsfrihet, och andra tillämpliga bestämmelser i unionsrätten, i synnerhet i fråga om skydd av personuppgifter, konkurrens och elektronisk handel.

2. Denna rekommendation bygger på och befäster de framsteg som har gjorts inom ramen för frivilliga överenskommelser mellan värdtjänstleverantörer och andra berörda tjänsteleverantörer i fråga om olika typer av olagligt innehåll. På området terrorism bygger den vidare på och befäster de framsteg som gjorts inom ramen för EU:s internetforum.

3. Rekommendationen ska inte påverka medlemsstaternas rättigheter och skyldigheter att vidta åtgärder avseende olagligt innehåll online enligt unionsrätten, inklusive möjligheten för medlemsstaternas domstolar eller administrativa myndigheter att i enlighet med sina rättssystem kräva att värdtjänstleverantörer avlägsnar eller blockerar olagligt innehåll. Denna rekommendation påverkar inte heller den ställning som värdtjänstleverantörer har enligt direktiv 2000/31/EG och deras möjlighet att fastställa och genomdriva sina användarvillkor i enlighet med unionslagstiftningen och medlemsstaternas lagstiftning.

([1]) Europaparlamentets och rådets direktiv (EU) 2016/680 av den 27 april 2016 om skydd för fysiska personer med avseende på behöriga myndigheters behandling av personuppgifter för att förebygga, förhindra, utreda, avslöja eller lagföra brott eller verkställa straffrättsliga påföljder, och det fria flödet av sådana uppgifter och om upphävande av rådets rambeslut 2008/977/RIF (EUT L 119, 4.5.2016, s. 89).

4. I denna rekommendation gäller följande definitioner:

a) *värdtjänstleverantör*: en leverantör av informationssamhällets tjänster som består av lagring av information som tillhandahållits av tjänstemottagaren på dennas begäran, i den mening som avses i artikel 14 i direktiv 2000/31/EG, vars verksamhet riktas till konsumenter som är bosatta i unionen, oavsett leverantörens etableringsort.

b) *olagligt innehåll*: information som inte är förenlig med unionslagstiftningen eller en berörd medlemsstats lagstiftning.

c) *användare*: en fysisk eller juridisk person som är mottagare av de tjänster som tillhandahålls av en värdtjänstleverantör.

d) *innehållsleverantör*: en användare som har lämnat information som på dennas begäran lagras eller har lagrats av en värdtjänstleverantör.

e) *anmälan*: kommunikation som riktas till en värdtjänstleverantör och som lämnas in av en anmälare avseende innehåll som lagras av den värdtjänstleverantören och som anmälaren anser vara olagligt innehåll, med begäran om att värdtjänstleverantören på frivillig basis ska avlägsna eller blockera innehållet.

f) *anmälare*: en person eller enhet som har lämnat en anmälan till en värdtjänstleverantör.

g) *betrodd anmälare*: en person eller enhet som enligt en värdtjänstleverantör har särskild sakkunskap och ett särskilt ansvar när det gäller att bekämpa olagligt innehåll på nätet.

h) *terrorisminnehåll*: information vars spridning innebär ett brott som anges i direktiv (EU) 2017/541 eller terroristbrott som anges i den berörda medlemsstatens lagstiftning, inklusive spridning av relevant information som produceras av eller kan hänföras till terroristgrupper eller enheter som ingår i de relevanta förteckningar som fastställs av unionen eller Förenta nationerna.

i) *brottsbekämpande myndigheter*: de myndigheter som av medlemsstaterna i enlighet med deras nationella lagstiftning har utsetts som behöriga att utföra brottsbekämpning i syfte att förebygga, utreda, upptäcka eller lagföra brott i samband med olagligt innehåll online.

j) *behöriga myndigheter*: de myndigheter som av medlemsstaterna i enlighet med deras nationella lagstiftning har utsetts som behöriga att utföra uppgifter som omfattar åtgärder mot olagligt innehåll online, bland annat brottsbekämpande myndigheter och förvaltningsmyndigheter som har i uppgift att verkställa lagstiftningen, oavsett arten av eller det särskilda sakinnehållet i lagstiftningen, tillämplig på vissa särskilda områden.

k) *hänskjutande*: kommunikation som riktas till en värdtjänstleverantör och som lämnas in av en behörig myndighet eller Europol avseende innehåll som lagras av den värdtjänstleverantören och som den myndigheten eller Europol anser vara terrorisminnehåll, med begäran om att värdtjänstleverantören på frivillig basis ska avlägsna eller blockera innehållet.

## KAPITEL II

## Allmänna rekommendationer avseende alla typer av olagligt innehåll

*Inlämning och handläggning av anmälningar*

5. Det bör inrättas mekanismer för att lämna in anmälningar. Dessa mekanismer bör vara lättillgängliga, användarvänliga och göra det möjligt att lämna in anmälningar elektroniskt.

6. Dessa mekanismer bör möjliggöra och uppmuntra till inlämning av anmälningar som är tillräckligt exakta och underbyggda för att den berörda värdtjänstleverantören ska kunna fatta ett välgrundat och omsorgsfullt beslut om det innehåll som anmälan rör, i synnerhet om innehållet är att betrakta som olagligt innehåll och ska avlägsnas eller blockeras. Dessa mekanismer bör vara sådana att de gör det lätt att lämna in anmälningar som innehåller en redogörelse för skälen till att anmälaren anser att innehållet är olagligt innehåll och en tydlig anvisning om var innehållet finns.

7. Anmälare bör ha möjlighet, men inte vara skyldiga, att lämna sina kontaktuppgifter i en anmälan. Om de beslutar att göra det bör deras anonymitet garanteras gentemot innehållsleverantören.

8. Om värdtjänstleverantören känner till anmälarens kontaktuppgifter bör värdtjänstleverantören sända ett mottagningsbevis till anmälaren och utan onödigt dröjsmål informera den senare på ett proportionerligt sätt om sitt beslut avseende det anmälda innehållet.

*Information till innehållsleverantörer och motanmälan*

9. Om en värdtjänstleverantör beslutar att avlägsna eller blockera innehåll som den lagrar eftersom den anser det vara olagligt innehåll, oavsett på vilket sätt innehållet har upptäckts, identifierats, avlägsnats eller blockerats, och om värdtjänstleverantören känner till innehållsleverantörens kontaktuppgifter, bör innehållsleverantören utan onödigt dröjsmål informeras på ett proportionerligt sätt om beslutet och skälen för det samt den möjlighet att bestrida beslutet som avses i punkt 11.

10. Punkt 9 ska dock inte gälla när det är uppenbart att innehållet är olagligt innehåll och rör allvarliga brott som innebär ett hot mot människors liv eller säkerhet. Dessutom bör värdtjänstleverantörer inte ge den information som avses i den punkten om och under så lång tid som en behörig myndighet begär detta av hänsyn till allmän ordning och säkerhet och i synnerhet för att förebygga, utreda, upptäcka och lagföra brott.

11. Innehållsleverantörer bör ges möjlighet att bestrida värdtjänstleverantörens beslut som avses i punkt 9 inom en rimlig tidsfrist genom inlämning av en motanmälan till den värdtjänstleverantören. Mekanismen för att lämna in en sådan motanmälan bör vara användarvänlig och möjliggöra inlämning på elektronisk väg.

12. Det bör säkerställas att värdtjänstleverantörer tar vederbörlig hänsyn till eventuella motanmälningar som de tar emot. Om motanmälan ger värdtjänstleverantören orsak att anse att det innehåll som motanmälan avser inte ska betraktas som olagligt innehåll bör den utan onödigt dröjsmål ändra sitt beslut att avlägsna eller blockera innehållet, utan att det påverkar dess möjlighet att fastställa och genomdriva sina användarvillkor i enlighet med unionslagstiftningen och medlemsstaternas lagstiftning.

13. Den innehållsleverantör som lämnade in en motanmälan, samt den berörda anmälaren, bör utan onödigt dröjsmål informeras om det beslut som värdtjänstleverantören har fattat avseende det berörda innehållet, om värdtjänstleverantören känner till deras kontaktuppgifter.

*Tvistlösning utanför domstol*

14. Medlemsstaterna uppmanas att när det är lämpligt underlätta tvistlösning utanför domstol för att lösa tvister i fråga om avlägsnande eller blockering av olagligt innehåll. Mekanismerna för tvistlösning utanför domstol bör vara lättillgängliga, effektiva, öppna och opartiska och bör säkerställa att lösningen är rättvis och stämmer överens med tillämplig lagstiftning. Försök att lösa sådana tvister utanför domstol bör inte påverka de berörda parternas tillgång till domstolsprövning.

15. Värdtjänstleverantörer uppmanas att tillåta användning av mekanismer för tvistlösning utanför domstol om sådana är tillgängliga i den berörda medlemsstaten.

*Öppenhet*

16. Värdtjänstleverantörer bör uppmuntras att offentliggöra tydliga, lättfattliga och tillräckligt detaljerade förklaringar om sin policy i fråga om att avlägsna eller blockera innehåll som de lagrar, inklusive innehåll som anses vara olagligt innehåll.

17. Värdtjänstleverantörer bör uppmuntras att regelbundet, helst minst en gång om året, offentliggöra rapporter om sin verksamhet i fråga om att avlägsna och blockera innehåll som anses vara olagligt innehåll. Rapporterna bör i synnerhet innehålla information om mängden och typen av innehåll som har avlägsnats, antalet anmälningar och motanmälningar som tagits emot samt hur länge det tagit att vidta åtgärder.

*Proaktiva åtgärder*

18. Värdtjänstleverantörer bör uppmuntras att vidta proportionerliga och särskilda proaktiva åtgärder mot olagligt innehåll, när detta är lämpligt. Sådana proaktiva åtgärder kan omfatta användning av automatiska verktyg för upptäckt av olagligt innehåll endast när det är lämpligt och proportionerligt och förutsatt att det finns effektiva och lämpliga skyddsåtgärder, i synnerhet de skyddsåtgärder som avses i punkterna 19 och 20.

*Skyddsåtgärder*

19. För att undvika avlägsnande av innehåll som inte är olagligt innehåll bör det, utan att det påverkar värdtjänstleverantörernas möjlighet att fastställa och genomdriva sina användarvillkor i enlighet med unionslagstiftningen och medlemsstaternas lagstiftning, finnas effektiva och lämpliga skyddsåtgärder för att säkerställa att värdtjänstleverantörer agerar på ett samvetsgrant och proportionerligt sätt med avseende på det innehåll som de lagrar, i synnerhet när de behandlar anmälningar och motanmälningar och när de fattar beslut om att avlägsna eller blockera innehåll som anses vara olagligt innehåll.

20. När värdtjänstleverantörer använder automatiska verktyg avseende det innehåll som de lagrar bör effektiva och lämpliga skyddsmekanismer vara tillgängliga för att se till att beslut som fattas angående detta innehåll, i synnerhet beslut om att avlägsna eller blockera innehåll som anses vara olagligt innehåll, är korrekta och välgrundade. Sådana skyddsåtgärder bör särskilt omfatta mänsklig övervakning och kontroll, när detta är lämpligt och i alla händelser när det krävs en detaljerad bedömning av det relevanta sammanhanget för att besluta om innehållet ska anses vara olagligt innehåll eller inte.

*Skydd mot missbruk*

21. Effektiva och lämpliga åtgärder bör vidtas för att förhindra inlämning av eller åtgärder till följd av anmälningar eller motanmälningar som lämnas in i ond tro och andra former av missbruk avseende de åtgärder som rekommenderas för att komma till rätta med olagligt innehåll online enligt denna rekommendation.

*Samarbete mellan värdtjänstleverantörer och medlemsstater*

22. Medlemsstaterna och värdtjänstleverantörerna bör utse kontaktpunkter för frågor som rör olagligt innehåll på nätet.

23. Påskyndade förfaranden bör inrättas för behandling av anmälningar som görs av behöriga myndigheter.

24. Medlemsstaterna uppmuntras att införa rättsliga skyldigheter för värdtjänstleverantörer att snabbt informera de brottsbekämpande myndigheterna, i syfte att förebygga, utreda, upptäcka eller lagföra brott, om belägg för påstådda allvarliga brott som innebär ett hot mot människors liv eller säkerhet och som erhållits inom ramen för deras verksamhet med att avlägsna eller blockera olagligt innehåll, i enlighet med tillämpliga rättsliga krav, i synnerhet gällande skyddet av personuppgifter, däribland förordning (EU) 2016/679.

*Samarbete mellan värdtjänstleverantörer och betrodda anmälare*

25. Samarbete mellan värdtjänstleverantörer och betrodda anmälare bör uppmuntras. I synnerhet bör påskyndade förfaranden inrättas för behandling av anmälningar som görs av betrodda anmälare.

26. Värdtjänstleverantörer bör uppmuntras att offentliggöra tydliga och objektiva villkor för hur de avgör vilka personer eller enheter de anser vara betrodda anmälare.

27. Dessa villkor bör syfta till att garantera att de berörda personerna eller enheterna har den sakkunskap som krävs och utför sina uppgifter som betrodda anmälare på ett samvetsgrant och objektivt sätt som grundar sig på respekt för de värden som unionen bygger på.

*Samarbete mellan värdtjänstleverantörer*

28. När det är lämpligt bör värdtjänstleverantörer utbyta erfarenheter, tekniska lösningar och bästa praxis i fråga om bekämpning av olagligt innehåll online med varandra och i synnerhet med värdtjänstleverantörer som på grund av sin storlek eller verksamhetens omfattning har begränsade resurser och sakkunskaper, även i samband med pågående samarbeten mellan värdtjänstleverantörer genom uppförandekoder, samförståndsavtal och andra frivilliga arrangemang.

## KAPITEL III

## Särskilda rekommendationer avseende terrorisminnehåll

*Allmänt*

29. De särskilda rekommendationer avseende terrorisminnehåll som fastställs i detta kapitel ska tillämpas utöver de allmänna rekommendationer som anges i kapitel II.

30. Värdtjänstleverantörer bör uttryckligen ange i sina användarvillkor att de inte kommer att lagra terrorisminnehåll.

31. Värdtjänstleverantörer bör vidta åtgärder så att de inte lagrar terrorisminnehåll, i synnerhet när det gäller hänskjutanden, proaktiva åtgärder och samarbete i enlighet med punkterna 32–40.

*Inlämning och handläggning av hänskjutanden*

32. Medlemsstaterna bör se till att de behöriga myndigheterna har förmågan och de nödvändiga resurserna att effektivt upptäcka och identifiera terrorisminnehåll och lämna hänskjutanden till de berörda värdtjänstleverantörerna, i synnerhet genom de nationella enheterna för anmälan av innehåll på internet och i samarbete med EU-enheten för anmälan av innehåll på internet vid Europol.

33. Det bör inrättas mekanismer för inlämning av hänskjutanden. Påskyndade förfaranden bör inrättas för behandling av hänskjutanden, i synnerhet hänskjutanden som inlämnats av de nationella enheterna för anmälan av innehåll på internet och EU-enheten för anmälan av innehåll på internet vid Europol.

34. Värdtjänstleverantörer bör utan onödigt dröjsmål sända bekräftelser på att de mottagit hänskjutandena och informera den behöriga myndigheten eller Europol om sitt beslut avseende det innehåll som avses och, i förekommande fall, uppge när innehållet avlägsnades eller blockerades eller varför de beslutade att inte avlägsna eller blockera innehållet.

35. Värdtjänstleverantörer bör som en allmän regel bedöma och, i tillämpliga fall, avlägsna eller blockera innehåll som anges i hänskjutandena inom en timme från den tidpunkt då de tog emot hänskjutandet.

*Proaktiva åtgärder*

36. Värdtjänstleverantörer bör vidta proportionerliga och särskilda proaktiva åtgärder, även med hjälp av automatiska verktyg, för att upptäcka, identifiera och snabbt avlägsna eller blockera terrorisminnehåll.

37. Värdtjänstleverantörer bör vidta proportionerliga och särskilda proaktiva åtgärder, även med hjälp av automatiska verktyg, för att omedelbart förhindra innehållsleverantören från att på nytt ladda upp innehåll som redan har avlägsnats eller blockerats eftersom det anses vara terrorisminnehåll.

*Samarbete*

38. För att förhindra att terrorisminnehåll sprids på flera värdtjänster bör värdtjänstleverantörer uppmuntras att samarbeta genom utbyte och optimering av effektiva, lämpliga och proportionerliga tekniska verktyg, även sådana verktyg som möjliggör automatisk upptäckt av innehåll. Om det är tekniskt möjligt bör alla relevanta format som används för att sprida terrorisminnehåll beaktas. Sådant samarbete bör framför allt inbegripa värdtjänstleverantörer som på grund av sin storlek eller verksamhetens omfattning har begränsade resurser och sakkunskaper.

39. Värdtjänstleverantörer bör uppmuntras att vidta nödvändiga åtgärder för att de verktyg som avses i punkt 38 ska fungera korrekt och förbättras, i synnerhet genom att fastställa identifierare avseende allt innehåll som anses vara terrorisminnehåll och genom att fullt ut utnyttja möjligheterna med dessa verktyg.

40. Behöriga myndigheter och värdtjänstleverantörer bör ingå samarbetsavtal, när det är lämpligt även med Europol, i ärenden som rör terrorisminnehåll på nätet, bland annat för att förbättra förståelsen av terroristverksamhet online, förbättra hänskjutandemekanismer, förhindra onödigt dubbelarbete och underlätta brottsbekämpande myndigheters begäranden för brottsutredningar som rör terrorism.

## KAPITEL IV

## Tillhandahållande av information

41. Medlemsstaterna bör regelbundet, helst var tredje månad, rapportera till kommissionen om de hänskjutanden som de berörda myndigheterna har gjort och de beslut som värdtjänstleverantören har fattat till följd av hänskjutandena, samt om deras samarbete med värdtjänstleverantörer kring bekämpning av terrorisminnehåll.

42. För att möjliggöra övervakning av hur denna rekommendation har omsatts i praktiken vad gäller terrorisminnehåll bör värdtjänstleverantörer, senast tre månader räknat från dagen för offentliggörandet, på kommissionens begäran tillställa den all information som behövs för en sådan övervakning. Denna information kan i synnerhet röra information om den mängd innehåll som har avlägsnats eller blockerats, antingen till följd av hänskjutanden eller anmälningar eller till följd av proaktiva åtgärder som har vidtagits och användning av automatiska verktyg. Den kan också inbegripa antalet hänskjutanden som tagits emot och den tid som har krävts för att vidta åtgärder, samt den mängd innehåll som har förhindrats från att laddas upp eller laddas upp på nytt genom användning av automatisk upptäckt av innehåll och andra tekniska verktyg.

43. För att möjliggöra övervakning av hur denna rekommendation har omsatts i praktiken vad gäller annat olagligt innehåll än terrorisminnehåll bör medlemsstaterna och värdtjänstleverantörer, senast sex månader räknat från dagen för offentliggörandet, på kommissionens begäran tillställa den all information som behövs för en sådan övervakning.

Utfärdad i Bryssel den 1 mars 2018.

*På kommissionens vägnar*

Andrus ANSIP

*Vice ordförande*