

# ПРЕПОРЪКИ

## ПРЕПОРЪКА (ЕС) 2018/334 НА КОМИСИЯТА

от 1 март 2018 година

### относно мерки за ефективна борба с незаконното съдържание онлайн

ЕВРОПЕЙСКАТА КОМИСИЯ,

като взе предвид Договора за функционирането на Европейския съюз, и по-специално член 292 от него,

като има предвид, че:

- (1) Интернет и доставчиците на услуги, осъществяващи дейност чрез интернет, имат съществен принос за иновациите, икономическия растеж и създаването на работни места в Съюза. Много от тези доставчици на услуги играят съществена роля в цифровата икономика, като свързват бизнеса и гражданите и улесняват обществените дебати и разпространяването и получаването на фактическа информация, мнения и идеи. В някои случаи обаче техните услуги стават обект на злоупотреби от страна на трети лица с цел извършване на незаконни дейности онлайн, като например разпространение на информация, свързана с тероризъм, сексуално насилие над деца, неправомерен език на омразата или нарушения на законодателството за защита на потребителите, като тези злоупотреби могат да подкопаят доверието на потребителите и да увредят бизнес моделите на тези доставчици на услуги. Понякога засегнатите доставчици на услуги може дори да извлекат някои предимства от такива дейности, например вследствие на наличието на защитено с авторско право съдържание, без да е дадено разрешение от носителите на права.
- (2) Наличността на незаконно съдържание онлайн води до сериозни отрицателни последици за потребителите, за други засегнати граждани и дружества, както и за обществото като цяло. Като се имат предвид централната им роля и технологичните средства и способности, свързани с предлаганите от тях услуги, доставчиците на онлайн услуги носят особени обществени отговорности да помагат за борбата с незаконното съдържание, разпространявано чрез използването на техните услуги.
- (3) С оглед на това, че бързото премахване на незаконното съдържание или блокирането на достъпа до него често са от съществено значение за ограничаването на по-широкото разпространение на това съдържание и причиняването на вреди, посочените отговорности предполагат, наред с другото, че засегнатите доставчици на услуги следва да могат да вземат бързи решения относно възможните действия спрямо незаконното съдържание онлайн. Тези отговорности предполагат също така, че доставчиците на услуги следва да въведат ефективни и подходящи гаранции, по-специално с цел осигуряване на надлежността и пропорционалността на своите действия и предотвратяване на неволното премахване на съдържание, което не е незаконно.
- (4) Много доставчици на услуги онлайн са признали тези отговорности и са предприели действия във връзка с тях. На колективно равнище бе постигнат значителен напредък посредством доброволни договорености от различно естество, сред които са Интернет форумът на ЕС за борба с терористичното съдържание онлайн, Кодексът за поведение относно противодействие на незаконния език на омразата онлайн и Меморандумът за разбирателство относно продажбата на фалшифицирани стоки по интернет. Въпреки тази ангажираност и напредък обаче незаконното съдържание онлайн продължава да бъде сериозен проблем в Съюза.
- (5) Загрижен поради серия от терористични нападения в ЕС и разпространението на терористична пропаганда онлайн, Европейският съвет от 22—23 юни 2017 г. заяви, че „очаква от [интернет индустрията] да [...] разработи [...] нови технологии и инструменти за подобряване на автоматичното откриване и премахване на съдържание, което подбужда към терористични нападения. ...“ В своята резолюция от 15 юни 2017 г. Европейският парламент призова настоятелно онлайн платформите „да засилят мерките за борба с незаконното и вредното онлайн съдържание“. Призивът към дружествата да възприемат по-проактивен подход при защитата на своите потребители от терористично съдържание бе повторно отправен и от министрите на държавите членки в рамките на Интернет форума на ЕС. Що се отнася до правата на интелектуална собственост, в заключенията си от 4 декември 2014 г. относно упражняването на тези права Съветът призова Комисията да разгледа използването на наличните инструменти за идентифициране на нарушителите на правата на интелектуална собственост и ролята на посредниците в подпомагането на борбата срещу нарушенията на правата на интелектуална собственост.

- (6) На 28 септември 2017 г. Комисията прие съобщение, съдържащо насоки във връзка с отговорността на доставчиците на услуги онлайн по отношение на незаконното онлайн съдържание <sup>(1)</sup>. В съобщението Комисията обясни, че ще прецени дали са необходими допълнителни мерки, като за целта ще проследи също така напредъка, постигнат въз основа на доброволните договорености. Настоящата препоръка е следствие от съобщението, като отразява степента на заложената в него амбиция и я реализира, надлежно отчитайки и укрепвайки съществуващия напредък, постигнат чрез доброволните договорености.
- (7) В настоящата препоръка се признава, че следва надлежно да се вземат под внимание както особеностите при борбата с различните видове незаконно съдържание онлайн, така и специфичните решения, които може да се изискват, включително приемането на специални законодателни мерки. Така например, признавайки необходимостта от такива специални законодателни мерки, Комисията прие на 25 май 2016 г. предложение за изменение на Директива 2010/13/ЕС на Европейския парламент и на Съвета <sup>(2)</sup> с оглед на променящите се пазарни условия. На 14 септември 2016 г. Комисията прие също така предложение за Директива относно авторското право в цифровия единен пазар <sup>(3)</sup>, в която се предвижда задължение за някои доставчици на услуги да предприемат в сътрудничество с носителите на права мерки за гарантиране на действието на споразуменията, сключени с носителите на права за използване на техни произведения или други обекти или за недопускане в техните услуги да се предлагат произведения или други обекти, идентифицирани от носителите на права в сътрудничество с доставчиците на услуги. Настоящата препоръка не засяга подобни законодателни мерки и предложения.
- (8) В Директива 2000/31/ЕО на Европейския парламент и на Съвета <sup>(4)</sup> се предвиждат възможности за освобождаване от отговорност, които при определени условия могат да се прилагат спрямо някои доставчици на услуги онлайн, в това число и доставчици на хостинг услуги по смисъла на член 14 от нея. За да се възползват от това освобождаване от отговорност, доставчиците на хостинг услуги трябва да действат експедитивно за отстраняване или блокиране на достъпа до съхраняваната от тях незаконна информация, след като узнаят за нея, а по отношение на искове за вреди — след като се запознаят с факти или обстоятелства, от които е видна незаконната дейност или информация. Те могат да получат такива сведения или да се запознаят с такива факти или обстоятелства и чрез подадени до тях сигнали за незаконно съдържание. Сама по себе си Директива 2000/31/ЕО представлява основанието за разработване на процедури за премахването на незаконна информация и блокирането на достъпа до такава информация. Директивата предвижда също така възможност държавите членки да изискват от засегнатите доставчици на услуги да действат с дължимата грижа във връзка с незаконно съдържание, което евентуално съхраняват.
- (9) При предприемане на мерки относно незаконното съдържание онлайн държавите членки трябва да спазват принципа на държавата на произход, установен в Директива 2000/31/ЕО. Съответно държавите членки не могат, по причини, свързани с координираната област по смисъла на тази директива, да ограничават свободата на предоставяне на услуги на информационното общество от доставчици, установени в друга държава членка, като обаче се запазва възможността за дерогации при определени условия, посочени в директивата.
- (10) Наред с това няколко други акта от правото на Съюза установяват правна уредба по отношение на някои конкретни видове незаконно съдържание, което е на разположение и се разпространява онлайн. По-специално съгласно Директива 2011/93/ЕС на Европейския парламент и на Съвета <sup>(5)</sup> от държавите членки се изисква да предприемат мерки за премахване на уебстраници, съдържащи или разпространяващи детска порнография, и им се позволява да блокират достъпа до такива уебстраници при установяване на определени гаранции. Директива (ЕС) 2017/541 на Европейския парламент и на Съвета <sup>(6)</sup>, която трябва да бъде транспонирана в националното право до 8 септември 2018 г., съдържа сходни разпоредби по отношение на онлайн съдържанието, представляващо публично подстрекаване към извършване на терористично престъпление. Директива (ЕС) 2017/541 установява също така минимални правила относно определението за престъпления в областта на терористичните престъпления, престъпленията, свързани с терористични групи, и престъпленията, свързани с терористични

<sup>(1)</sup> COM(2017) 555 final, 28 септември 2017 г.

<sup>(2)</sup> Директива 2010/13/ЕС на Европейския парламент и на Съвета от 10 март 2010 година за координирането на някои разпоредби, установени в закони, подзаконови и административни актове на държавите-членки, отнасящи се до предоставянето на аудиовизуални медийни услуги (Директива за аудиовизуалните медийни услуги) (ОВ L 95, 15.4.2010 г., стр. 1). COM(2016) 287 final.

<sup>(3)</sup> COM(2016) 593 final, 14 септември 2016 г.

<sup>(4)</sup> Директива 2000/31/ЕО на Европейския парламент и на Съвета от 8 юни 2000 г. за някои правни аспекти на услугите на информационното общество, и по-специално на електронната търговия на вътрешния пазар (Директива за електронната търговия) (ОВ L 178, 17.7.2000 г., стр. 1).

<sup>(5)</sup> Директива 2011/93/ЕС на Европейския парламент и на Съвета от 13 декември 2011 г. относно борбата със сексуалното насилие и със сексуалната експлоатация на деца, както и с детската порнография и за замяна на Рамково решение 2004/68/ПВР на Съвета (ОВ L 335, 17.12.2011 г., стр. 1).

<sup>(6)</sup> Директива (ЕС) 2017/541 на Европейския парламент и на Съвета от 15 март 2017 г. относно борбата с тероризма и за замяна на Рамково решение 2002/475/ПВР на Съвета, и за изменение на Решение 2005/671/ПВР на Съвета (ОВ L 88, 31.3.2017 г., стр. 6).

дейности. Съгласно Директива 2004/48/ЕО на Европейския парламент и на Съвета <sup>(1)</sup> компетентните съдебни органи могат да постановяват забрани срещу посредниците, чиито услуги се използват от трета страна за нарушаване на право върху интелектуална собственост.

- (11) В този контекст по-специално и в допълнение към доброволните мерки, предприети от някои доставчици на услуги онлайн, след приемането на Директива 2000/31/ЕО някои държави членки приеха разпоредби относно механизмите за уведомяване и предприемане на действия. Други държави членки възнамеряват да приемат такива разпоредби. По принцип въпросните механизми имат за цел да улеснят уведомяването на засегнатия доставчик на хостинг услуги за наличието на съдържание, което уведомящата страна счита за незаконно („уведомяване“), вследствие на което доставчикът може да реши дали е съгласен с преценката на уведомяващия и дали желае да премахне въпросното съдържание или да блокира достъпа до него („действие“). Между тези национални разпоредби има все по-големи различия. В резултат на това засегнатите доставчици на услуги могат да бъдат задължени да спазват редица нормативни изисквания, различаващи се по своето съдържание и обхват.
- (12) В интерес на вътрешния пазар и на ефективността при борбата с незаконното съдържание онлайн и за да се запази балансираният подход, който Директива 2000/31/ЕО има за цел да осигури, е необходимо да се установят някои основни принципи, от които да се ръководят дейностите на държавите членки и на засегнатите доставчици на услуги в тази насока.
- (13) Тези принципи следва да се установят и прилагат при пълно зачитане на основните права, защитавани в правния ред на Съюза, и по-специално на основните права, гарантирани в Хартата на основните права на Европейския съюз (наричана по-нататък „Хартата“). Борбата с незаконното съдържание онлайн следва да се води чрез предвиждане на подходящи и сериозни гаранции, за да се осигури защита на различните изложени на опасност основни права на всички засегнати страни. В зависимост от случая тези права включват свободата на изразяване на мнение, в това число и свободата да се получава и разпространява информация, правото на зачитане на личния живот, правото на защита на личните данни, както и правото на ефективна съдебна защита на потребителите на засегнатите услуги. Тези права могат да включват също свободата на стопанската инициатива, в това число и свободата на договаряне, на доставчиците на хостинг услуги, както и правата на детето и правата на защита на собствеността, включително на интелектуалната собственост, правото на човешко достойнство и правото на недискриминация на някои други засегнати страни. По-специално, когато доставчиците на хостинг услуги вземат решения за премахване на съхранявано от тях съдържание или за блокиране на достъпа до такова съдържание, те следва да вземат надлежно под внимание основните права и законните интереси на своите потребители, както и централната роля, която самите доставчици обикновено играят за улесняване на обществения дебат и за разпространяването и възприемането на факти, мнения и идеи при спазване на закона.
- (14) Съгласно хоризонталния подход, залегнал в основата на освобождаването от отговорност, предвидено в член 14 от Директива 2000/31/ЕО, настоящата препоръка следва да се прилага за всеки вид съдържание, което не е в съответствие с правото на Съюза или с правото на държавите членки, независимо от конкретния предмет или естеството на съответното право. Достатъчно е да се вземе под внимание правото на държавите членки, засегнати от съответното предоставяне на услуги, и по-конкретно правото на държавите членки, на чиято територия е установен доставчикът на хостинг услуги или на чиято територия се предоставят услугите. Освен това при привеждане в действие на настоящата препоръка следва надлежно да се вземат под внимание степента на тежест на незаконното съдържание, всички видове вреди, които могат да бъдат причинени от него — тези два елемента могат да бъдат тясно свързани с бързината на предприеманите действия — и онова, което може основателно да се очаква от доставчиците на хостинг услуги, като по целесъобразност се вземат предвид степента на развитие на технологиите и възможната им употреба. Също така следва да се отчитат релевантните различия, които може да съществуват между различните видове незаконно съдържание и действията, които следва да се предприемат за борба с това съдържание.
- (15) Доставчиците на хостинг услуги играят особено важна роля в борбата с незаконното съдържание онлайн, тъй като те съхраняват информация, предоставена от техните потребители, по искане на тези потребители и предоставят на други потребители достъп до нея, често в голям мащаб. Поради това настоящата препоръка се отнася преди всичко за дейностите и отговорностите на тези доставчици. Когато е уместно обаче, отправените препоръки може да се прилагат *mutatis mutandis* и по отношение на други засегнати доставчици на услуги онлайн. Тъй като целта на настоящата препоръка е да се предприемат действия във връзка с рисковете, свързани с незаконното съдържание онлайн, засягащо потребителите в Съюза, тя се отнася за дейностите на всички доставчици на хостинг услуги, независимо дали те са установени в Съюза или в трета държава, при условие че дейностите им са насочени към потребители, пребиваващи в Съюза.
- (16) Механизмите за подаване на сигнали за незаконно съдържание до доставчиците на хостинг услуги във връзка със съдържание, смятано за незаконно, са важно средство за борба с незаконното съдържание онлайн. Тези механизми следва да улесняват подаването на сигнали от всички физически лица или образувания, желаещи да подадат

<sup>(1)</sup> Директива 2004/48/ЕО на Европейския парламент и на Съвета от 29 април 2004 г. относно упражняването на права върху интелектуалната собственост (ОВ L 157, 30.4.2004 г., стр. 45).

сигнал. По тази причина въпросните механизми следва да са лесно достъпни и лесни за ползване от всички потребители. Въпреки това доставчиците на хостинг услуги следва да запазят гъвкавост, например що се отнася до формата за съобщаване или технологията, които ще бъдат използвани, така че да се даде възможност за намиране на ефикасни решения и да се избегнат непропорционални тежести за тези доставчици.

- (17) Съгласно съдебната практика на Съда на ЕС във връзка с член 14 от Директива 2000/31/ЕО сигналите за незаконно съдържание следва да бъдат достатъчно точни и адекватно обосновани, за да може получаващият ги доставчик на хостинг услуги да вземе информирано и надлежно решение относно действията, които да бъдат предприети по сигнала. Следователно изпълнението на това изискване следва да се гарантира в колкото се може по-голяма степен. Дали обаче даден сигнал за незаконно съдържание води до получаване на сведения или запознаване с факти по смисъла на член 14 от Директивата ще се преценява с оглед на особеностите на конкретния случай, като се взема предвид, че получаването на тези сведения или запознаването с фактите може да стане и по други начини освен чрез сигнали за незаконно съдържание.
- (18) Получаването на координатите за връзка на подателя на сигнала за незаконно съдържание обикновено не е необходимо, за да може доставчикът на хостинг услуги да вземе информирано и надлежно решение за последващите действия, които да бъдат предприети по получения сигнал. Въвеждането на изискване за предоставяне на координати за връзка като предпоставка за подаване на сигнал за незаконно съдържание би създавало пречка за подаването на сигнали. Посочването на координатите за връзка обаче е необходимо, за да може доставчикът на хостинг услуги да предостави обратна информация. Следователно посочването на координатите за връзка следва да е възможност за подателя на сигнала, без обаче да е негово задължение.
- (19) За да се увеличат прозрачността и точността на механизмите за уведомяване и предприемане на действия и да се даде възможност за вземане на мерки за правна защита, когато това е необходимо, доставчиците на хостинг услуги следва да информират своевременно и по подходящ начин подателя на сигнала за незаконно съдържание и/или доставчика на съдържание, ако разполагат с координатите за връзка с тях, относно мерките, предприети в контекста на посочените механизми, и по-специално относно решенията си по исканията за премахване на съответното съдържание или за блокиране на достъпа до него. Предоставяната информация следва да е пропорционална, така че да съответства на изявленията на засегнатите лица, направени в подадените от тях сигнали за незаконно съдържание или възражения срещу такива сигнали, и същевременно да дава възможност за подходящи и диференцирани решения, без да води до прекомерна тежест за доставчиците.
- (20) За да се осигурят прозрачност и справедливост и да се избегне неволното премахване на съдържание, което не е незаконно съдържание, на доставчиците на съдържание следва по принцип да се предоставя информация за решението за премахване или блокиране на достъпа до съдържанието, съхранявано по тяхно искане, и да им се дава възможност да оспорят решението чрез възражение срещу сигнала за незаконно съдържание с цел постигане на оттегляне на решението, когато това е уместно, независимо дали въпросното решение е било взето въз основа на сигнал за незаконно съдържание или на сигнал за терористично съдържание или вследствие на проактивни мерки от страна на доставчика на хостинг услуги.
- (21) При все това, предвид естеството на въпросното съдържание, както и предвид целта на една такава процедура за подаване на възражения срещу сигнали за незаконно съдържание и допълнителната тежест, която тя поражда за доставчиците на хостинг услуги, няма основание да се препоръча предоставяне на такава информация за взетото решение и за възможността за оспорване на решението, когато е очевидно, че въпросното съдържание е незаконно и е свързано с тежки престъпления, при които има заплаха за живота или безопасността на хората, като например престъпленията, посочени в Директива (ЕС) 2017/541 и Директива 2011/93/ЕС. Освен това в определени случаи наличието на съображения, свързани с обществения ред и обществената сигурност, и по-специално съображения, свързани с предотвратяването, разследването, разкриването и наказателното преследване на престъпления, може да обоснове тази информация да не се предостави пряко на съответния доставчик на съдържание. Поради това доставчиците на хостинг услуги не следва да предоставят информацията, ако компетентен орган е отправил искане в този смисъл по съображения, свързани с обществения ред и обществената сигурност, за периода, поискан от въпросния орган с оглед на тези съображения. Доколкото това води до ограничаване на правото на информация по отношение на обработването на лични данни, следва да се спазват съответните изисквания, предвидени в Регламент (ЕС) 2016/679 на Европейския парламент и на Съвета <sup>(1)</sup>.
- (22) Механизмите за уведомяване и предприемане на действия не следва по никакъв начин да засягат правата на засегнатите страни да започнат съдебно производство съгласно приложимото право по повод съдържание, което се счита за незаконно, или по повод мерки, предприети в тази връзка от доставчиците на хостинг услуги. Механизмите за извънсъдебно уреждане на спорове, възникващи във връзка с това, могат да бъдат важно допълнение към съдебните производства, особено когато дават възможност за ефективно, финансово достъпно и бързо решаване на тези спорове. Поради това извънсъдебното уреждане на спорове следва да се насърчава, при условие че съответните механизми отговарят на определени стандарти, по-специално що се отнася до процесуалната справедливост, както и при условие че достъпът на страните до съд бъде запазен и че се избягват злоупотребни.

<sup>(1)</sup> Регламент (ЕС) 2016/679 на Европейския парламент и на Съвета от 27 април 2016 г. относно защитата на физическите лица във връзка с обработването на лични данни и относно свободното движение на такива данни и за отмяна на Директива 95/46/ЕО (Общ регламент относно защитата на данните) (ОВ L 119, 4.5.2016 г., стр. 1).

- (23) С оглед на по-доброто преценяване на ефективността на механизмите за уведомяване и предприемане на действия и на другите дейности на доставчиците на хостинг услуги във връзка със съдържанието, което се счита за незаконно, и за да се гарантира отчетност, следва да има прозрачност спрямо широката общественост. Поради това доставчиците на хостинг услуги следва редовно да публикуват доклади относно тези механизми и други дейности, като докладите следва да бъдат достатъчно пълни и изчерпателни, за да се даде възможност за получаване на подходяща представа. Доставчиците на хостинг услуги следва също така предварително да дават яснота, в своите условия за ползване на услугата, относно политиката си за премахване на съхраняваното от тях съдържание, включително незаконно съдържание, или за блокиране на достъпа до такова съдържание.
- (24) В допълнение към механизмите за уведомяване и предприемане на действия, доброволното вземане на пропорционални и конкретни проактивни мерки от страна на доставчиците на хостинг услуги, включително чрез използване на автоматизирани средства в някои случаи, също може да бъде важен елемент в борбата с незаконното съдържание онлайн, без да се засяга член 15, параграф 1 от Директива 2000/31/ЕО. Във връзка с тези проактивни мерки следва да се вземат под внимание както положението на доставчиците на хостинг услуги, които поради размера си или мащаба, в който работят, разполагат с ограничени ресурси и експертен опит, така и необходимостта от ефективни и подходящи гаранции, които да придружават тези мерки.
- (25) По-специално може да е уместно такива проактивни мерки да се вземат, когато незаконният характер на съдържанието е вече установен или когато съдържанието е от такъв вид, че поставянето му в даден контекст не е от съществено значение. Вземането на подобни мерки може да зависи също така от тяхното естество, мащаб и цел, от вида на съответното съдържание, от това дали правоприлагащите органи или Европол са подали сигнал за съдържанието и дали във връзка със съдържанието вече са предприети действия, тъй като то се смята за незаконно. Що се отнася конкретно до материалите, касаещи сексуално насилие над деца, доставчиците на хостинг услуги следва да вземат проактивни мерки за разкриване и предотвратяване на разпространението на такива материали, в съответствие с ангажиментите, поети в контекста на Глобалния алианс срещу сексуалното насилие над деца онлайн.
- (26) В този контекст в съобщението си от 28 септември 2017 г. относно борбата с незаконното онлайн съдържание Комисията изложи мнението си, че предприемането на такива доброволни проактивни мерки не води автоматично до невъзможност за съответния доставчик на хостинг услуги да се ползва от освобождаването от отговорност, предвидено в член 14 от Директива 2000/31/ЕО.
- (27) От съществено значение е във връзка с всички мерки за борба с незаконното съдържание онлайн да бъдат предвидени ефективни и подходящи гаранции, с които се цели осигуряване на надлежност и пропорционалност на действията на доставчиците на хостинг услуги, когато определят и прилагат политиката си спрямо съдържанието, което съхраняват, включително незаконното съдържание, така че да се гарантира по-специално, че потребителите могат свободно да получават и разпространяват информация онлайн в съответствие с приложимото право. В допълнение към евентуалните гаранции, регламентирани в приложимото право, например във връзка със защитата на личните данни, по отношение на използването на автоматизирани средства следва по целесъобразност да се предвиждат и прилагат специални гаранции, и по-конкретно човешки контрол и проверки, за да се избегне вземането на неволни и погрешни решения.
- (28) Между компетентните органи и доставчиците на хостинг услуги следва да се осигури лесно, ефективно и подходящо сътрудничество в борбата с незаконното съдържание онлайн. Това сътрудничество би могло да бъде подпомогнато от Европол, когато е целесъобразно, например при борбата с тероризма и сексуалното насилие и сексуалната експлоатация на деца, с детската порнография и с установяването на контакт с деца за сексуални цели. За да се улесни това сътрудничество, държавите членки и доставчиците на хостинг услуги следва да определят звена за контакт и следва да се въведат процедури за приоритетно разглеждане на сигналите за незаконно съдържание, подавани от компетентните органи, като се отдава подходяща степен на доверие в точността на сигналите предвид конкретните експертни познания и отговорности на въпросните органи. С оглед постигането на ефективност в борбата с някои особено тежки престъпления, като например посочените в Директива (ЕС) 2017/541 и Директива 2011/93/ЕС, за които доставчиците на хостинг услуги могат да узнаят при осъществяване на дейността си, държавите членки следва да бъдат насърчавани да използват предвидената в член 15, параграф 2 от Директива 2000/31/ЕО възможност за нормативно въвеждане на задължения за докладване при спазване на приложимото право, и по-специално на Регламент (ЕС) 2016/679.
- (29) Наред с компетентните органи някои физически лица или образувания, в това число и неправителствени организации и търговски сдружения, може също да разполагат с особени експертни познания и да желаят да поемат доброволно отговорности във връзка с борбата с незаконното съдържание онлайн. Предвид добавената им стойност и понякога големия брой подадени сигнали за незаконно съдържание, сътрудничеството между такива доверени податели на сигнали за незаконно съдържание и доставчиците на хостинг услуги следва да се насърчава, по-специално чрез приоритетно разглеждане на подадените от тях сигнали и отдаване на подходяща степен на доверие в точността на сигналите. При все това, в съответствие с конкретния им статут, такова сътрудничество

следва да е възможно само с физическите лица и образуванията, зачитащи установените в член 2 от Договора за Европейския съюз ценности, на които се основава Съюзът, и отговарящи на определени подходящи условия, като тези условия следва да бъдат ясни и обективни и да са обществено достояние.

- (30) Борбата с незаконното съдържание онлайн изисква да се възприеме цялостен подход, тъй като този вид съдържание често мигрира лесно от един доставчик на хостинг услуги към друг и при него се наблюдава тенденция за използване на най-слабите звена от веригата. По тази причина сътрудничеството, изразяващо се по-специално в доброволно споделяне на опит, технологични решения и най-добри практики, е от първостепенно значение. Това сътрудничество е особено важно за доставчиците на хостинг услуги, които поради своя размер или мащаба, в който работят, разполагат с ограничени ресурси и експертни познания.
- (31) Тероризмът е свързан с неправомерната и безразборна употреба на насилие и сплашване срещу гражданите. Терористите разчитат все повече на интернет за разпространяването на терористична пропаганда, като често използват сложни методи, за да осигурят нейното бързо и широко разпространение. Макар да е постигнат напредък, особено в контекста на Интернет форума на ЕС, все още има спешна нужда от по-бързи и по-ефективни действия срещу терористичното съдържание онлайн в допълнение към необходимостта доставчиците на хостинг услуги, участващи в Интернет форума на ЕС, да изпълняват изцяло ангажиментите си, свързани с ефективното и цялостно докладване.
- (32) С оглед на особеностите, свързани с борбата с терористичното съдържание онлайн, общите препоръки относно борбата с незаконното съдържание следва да бъдат допълнени с някои препоръки, отнасящи се специално за борбата с терористичното съдържание онлайн, като за целта се използва и консолидира постигнатото в резултат на усилията, положени в рамките на Интернет форума за ЕС.
- (33) Като се имат предвид особено сериозните рискове, свързани с терористичното съдържание, и централната роля на доставчиците на хостинг услуги при разпространението на подобно съдържание, доставчиците на хостинг услуги следва да предприемат всички разумни мерки, за да не допускат терористично съдържание и при възможност да предотвратяват неговия хостинг, като следва да се запазва възможността те да определят условията за ползване на предлаганите от тях услуги и да осигуряват спазването на тези условия, при отчитане на необходимостта от ефективни и подходящи гаранции и без да се засяга член 14 от Директива 2000/31/ЕО.
- (34) Посочените мерки следва в частност да се изразяват в сътрудничество с компетентните органи и Европол във връзка със сигналите за терористично съдържание, представляващи специално средство за уведомяване на доставчиците на хостинг услуги, адаптирано към особеностите на борбата с терористичното съдържание. При подаването на сигнали за терористично съдържание компетентните органи и Европол следва да могат да поискат премахването на съдържание, което те считат за терористично, или блокирането на достъпа до такова съдържание, позовавайки се на съответното приложимо право или на условията за ползване на услугата на съответния доставчик на хостинг услуги. Тези механизми за подаване на сигнали за терористично съдържание следва да съществуват в допълнение към механизмите за подаване на сигнали за незаконно съдържание, включително от доверени податели на сигнали за незаконно съдържание. Механизмите за подаване на сигнали за незаконно съдържание могат да се използват и за съобщаване за наличие на съдържание, считано за терористично съдържание.
- (35) Като се има предвид, че терористичното съдържание обикновено е най-вредно през първия час на неговото появяване онлайн и предвид специфичните експертни познания и отговорности на компетентните органи и Европол, разглеждането на сигналите за терористично съдържание и предприемането при необходимост на действия в отговор на тях следва да се извършват по правило в рамките на един час.
- (36) Без да се засяга член 15, параграф 1 от Директива 2000/31/ЕО мерките за борба с терористичното съдържание следва да включват също така пропорционални и специфични проактивни мерки, осъществявани включително чрез използване на автоматизирани средства, с цел откриване, идентифициране и бързо премахване на терористичното съдържание или блокиране на достъпа до него, както и с оглед да се гарантира, че терористичното съдържание няма да се появи отново. В това отношение следва да се вземе предвид необходимостта от адекватни и ефективни гаранции, които да съпътстват тези мерки, и по-специално гаранциите, които са препоръчани в глава II от настоящата препоръка.
- (37) Сътрудничеството, както между доставчиците на хостинг услуги, така и между тях и компетентните органи, е от изключително значение при воденето на борба с терористичното съдържание онлайн. По-специално, технологичните инструменти, които позволяват автоматизирано откриване на съдържание, като например базата данни с кодове за сегментиране (хеш-база данни), могат да помогнат да се постигне целта за предотвратяване на разпространението на терористично съдържание в различните хостинг услуги. Това сътрудничество, както и разработването, експлоатацията и споделянето на такива технологични инструменти следва да бъдат насърчавани, като при необходимост се използват експертните познания на Европол. Тези съвместни усилия са особено важни, за да се помогне на онези доставчици на хостинг услуги, които поради своя размер или мащаба, в който работят, разполагат с ограничени ресурси и експертни познания за предприемане на ефективни и спешни действия в отговор на сигналите за терористично съдържание и за вземане на проактивните мерки, които се препоръчват.

- (38) Колкото се може повече доставчици на хостинг услуги следва да се включат в тези съвместни усилия и всички участващи доставчици на хостинг услуги следва да допринасят за оптимизирането и максималното увеличаване на използването на тези инструменти. Сключването на работни договорености между всички съответни страни, включително, когато това е уместно, с Европол, също следва да бъде насърчавано, като се има предвид, че такива договорености могат да способстват за гарантиране на последователен и ефективен подход и да дадат възможност за обмен на опит и експертни познания.
- (39) С цел да се гарантират зачитането на основното право на защита на физическите лица във връзка с обработването на лични данни, както и свободното движение на лични данни, обработването на лични данни в контекста на мерките, предприети за изпълнение на настоящата препоръка, следва да бъде в пълно съответствие с правилата за защита на личните данни, по-специално с Регламент (ЕС) 2016/679 и Директива (ЕС) 2016/680 на Европейския парламент и на Съвета <sup>(1)</sup>, и следва да се наблюдава от компетентните надзорни органи.
- (40) В настоящата препоръка се зачитат основните права и се съблюдават принципите, признати по-специално в Хартата. По-специално, настоящата препоръка има за цел да гарантира пълното зачитане на членове 1, 7, 8, 10, 11, 16, 17, 21, 24 и 47 от Хартата.
- (41) Комисията възнамерява да наблюдава отблизо всички действия, предприети в отговор на настоящата препоръка. Ето защо държавите членки и доставчиците на хостинг услуги следва да бъдат готови да предоставят на Комисията, по нейно искане, цялата необходима информация, която може основателно да се очаква да предоставят, за да дадат възможност за осъществяването на това наблюдение. Въз основа на така получената информация и цялата друга налична информация, включително информацията от докладване въз основа на различните доброволни договорености, Комисията ще извърши оценка на изпълнението на настоящата препоръка, и ще прецени дали са необходими допълнителни мерки, включително изготвяне на предложения за обвързващи правни актове на Съюза. Като се имат предвид особеностите и спешният характер на борбата с терористичното съдържание онлайн, наблюдението и оценката следва да се извършат въз основа на подробна информация и особено бързо, в срок от три месеца от датата на публикуване на настоящата препоръка, а що се отнася до другото незаконно съдържание, е удачно те да се извършат в срок от шест месеца от датата на нейното публикуване.

ПРИЕ НАСТОЯЩАТА ПРЕПОРЪКА:

## ГЛАВА I

### Цел и терминология

1. Държавите членки, от една страна, и доставчиците на хостинг услуги, от друга — що се отнася до съхраняването от тях съдържание, предоставено от доставчици на съдържание, което се съхранява по искане на доставчиците на съдържание, — се насърчават да предприемат ефективни, подходящи и пропорционални мерки за борба с незаконното съдържание онлайн в съответствие с принципите, установени в настоящата препоръка, и при пълно спазване на Хартата, и по-специално на правото на свобода на изразяване на мнение и на правото на свобода на информацията, както и при спазване на другите приложими разпоредби на правото на Съюза, отнасящи се по-специално до защитата на личните данни, конкуренцията и електронната търговия.
2. Настоящата препоръка има за основа напредъка, постигнат в рамките на доброволните договорености, сключени между доставчиците на хостинг услуги и другите засегнати доставчици на услуги във връзка с различните видове незаконно съдържание, и укрепва този напредък. В областта на тероризма тя има за основа и укрепва напредъка, постигнат в рамките на Интернет форума на ЕС.
3. Настоящата препоръка не засяга правата и задълженията на държавите членки да предприемат мерки по отношение на незаконното съдържание онлайн в съответствие с правото на Съюза, включително възможността за съдилищата или административните органи на държавите членки да изискват, в съответствие със своите правни системи, от доставчиците на хостинг услуги да премахват незаконно съдържание или да блокират достъпа до него. Настоящата препоръка не засяга също така положението на доставчиците на хостинг услуги съгласно Директива 2000/31/ЕО и възможността им да определят условията си за ползване на услугата и да осигуряват спазването на тези условия в съответствие с правото на Съюза и правото на държавите членки.

<sup>(1)</sup> Директива (ЕС) 2016/680 на Европейския парламент и на Съвета от 27 април 2016 г. относно защитата на физическите лица във връзка с обработването на лични данни от компетентните органи за целите на предотвратяването, разследването, разкриването или наказателното преследване на престъпления или изпълнението на наказания и относно свободното движение на такива данни, и за отмяна на Рамково решение 2008/977/ПВР на Съвета (ОВ L 119, 4.5.2016 г., стр. 89).

4. За целите на настоящата препоръка се използват следните термини:
- а) „доставчик на хостинг услуги“ означава доставчик на услуги на информационното общество, състоящи се в съхраняване по молба на получателя на услугата на предоставена от него информация по смисъла на член 14 от Директива 2000/31/ЕО, който доставчик, независимо от мястото си на установяване, насочва дейностите си към потребители, пребиваващи в Съюза;
  - б) „незаконно съдържание“ означава всяка информация, която не е в съответствие с правото на Съюза или правото на съответната държава членка;
  - в) „потребител“ означава всяко физическо или юридическо лице, което е получател на услугите, предоставяни от доставчик на хостинг услуги;
  - г) „доставчик на съдържание“ означава потребител, предоставил информация, която се съхранява или е била съхранявана по негова молба от доставчик на хостинг услуги;
  - д) „сигнал за незаконно съдържание“ означава всяко съобщение, адресирано до доставчик на хостинг услуги и подадено от подател на сигнал за незаконно съдържание във връзка със съхраняване от този доставчик на хостинг услуги съдържание, считано за незаконно от подателя на сигнала за незаконно съдържание, с искане доставчикът на хостинг услуги доброволно да премахне това съдържание или да блокира достъпа до него;
  - е) „подател на сигнал за незаконно съдържание“ означава физическо лице или образувание, което е подало сигнал за незаконно съдържание до доставчик на хостинг услуги;
  - ж) „доверен подател на сигнал за незаконно съдържание“ означава физическо лице или образувание, за което доставчиците на хостинг услуги считат, че притежава специфични експертни познания и отговорности за целите на борбата с незаконното съдържание онлайн;
  - з) „терористично съдържание“ означава всяка информация, чието разпространение представлява престъпление, предвидено в Директива (ЕС) 2017/541, или терористично престъпление, предвидено в правото на съответната държава членка, включително разпространението на съответна информация, която е изготвена или се счита, че е изготвена от терористични групи или образувания, включени в съответните списъци, установени от Съюза или от Организацията на обединените нации;
  - и) „правоприлагащи органи“ означава компетентните органи, определени от държавите членки в съответствие с националното им право да изпълняват правоприлагащи функции за целите на предотвратяването, разследването, разкриването или наказателното преследване на престъпления във връзка с незаконното съдържание онлайн;
  - й) „компетентни органи“ означава компетентните органи, определени от държавите членки в съответствие с тяхното национално право да извършват задачи, сред които е борбата с незаконното съдържание онлайн, включително правоприлагащите и административните органи, които отговарят за осигуряване на спазването на законодателството, приложимо в някои конкретни области, независимо от естеството или специфичния предмет на това законодателство;
  - к) „сигнал за терористично съдържание“ означава всяко съобщение, адресирано до доставчик на хостинг услуги и подадено от компетентен орган или от Европол във връзка със съхраняване от този доставчик на хостинг услуги съдържание, считано за терористично от въпросния компетентен орган или Европол, с искане доставчикът на хостинг услуги доброволно да премахне това съдържание или да блокира достъпа до него.

## ГЛАВА II

### Общи препоръки, отнасящи се до всички видове незаконно съдържание

#### *Подаване и разглеждане на сигнали за незаконно съдържание*

5. Следва да се предвидят механизми за подаване на сигнали за незаконно съдържание. Тези механизми следва да са лесно достъпни, да са удобни за ползване и да предоставят възможност за подаване на сигнали за незаконно съдържание по електронен път.
6. Тези механизми следва да позволяват и насърчават подаването на сигнали за незаконно съдържание, които са достатъчно точни и адекватно обосновани, за да може съответният доставчик на хостинг услуги да вземе информирано и надлежно решение относно съдържанието, за което се отнася сигналът, и по-специално дали това съдържание трябва да се счита за незаконно и съответно да се премахне или достъпът до него да се блокира. Тези механизми следва да улесняват подаването на сигнали за незаконно съдържание, съдържащи обяснение на причините, поради които подателят на сигнала счита, че съдържанието е незаконно, както и ясно указание за местонахождението на това съдържание.



7. Подателите на сигнали за незаконно съдържание следва да имат възможността, но не и задължението, да включат в сигнала за незаконно съдържание своите координати за връзка. Ако те решат да направят това, следва да бъде осигурена тяхната анонимност спрямо доставчика на съдържание.
8. Когато координатите за връзка на подателя на сигнал за незаконно съдържание са известни на доставчика на хостинг услуги, доставчикът следва да изпрати на подателя потвърждение за получаването на сигнала за незаконно съдържание и следва своевременно да го информира по пропорционален начин за решението си по отношение на съдържанието, за което се отнася сигналът за незаконно съдържание.

#### *Информлиране на доставчиците на съдържание и възражения срещу сигналите за незаконно съдържание*

9. Когато доставчик на хостинг услуги вземе решение да премахне съдържание, което съхранява, или да блокира достъпа до такова съдържание, тъй като смята, че съдържанието е незаконно, независимо от използваното средство за откриване, идентифициране или премахване на съдържанието или за блокиране на достъпа до него, и когато координатите за връзка на доставчика на съдържанието са известни на доставчика на хостинг услуги, доставчикът на съдържанието следва да бъде информиран своевременно и по пропорционален начин за това решение и за причините, поради които то е взето, както и за посочената в точка 11 възможност да оспори това решение.
10. Точка 9 обаче не следва да се прилага, когато е очевидно, че въпросното съдържание е незаконно и е свързано с тежки престъпления, при които съществува заплахата за живота или безопасността на хората. Освен това, ако бъде отправено искане от компетентен орган по причини, свързани с обществения ред и обществената сигурност, и по-специално с предотвратяването, разследването, разкриването и наказателното преследване на престъпления, доставчиците на хостинг услуги следва да не предоставят информацията, посочена в тази точка, докато органът не им позволи.
11. На доставчиците на съдържание следва да бъде дадена възможност да оспорят в разумен срок решението на доставчика на хостинг услуги, посочено в точка 9, чрез подаване на възражение срещу сигнала за незаконно съдържание до този доставчик на хостинг услуги. Механизмът за подаване на такива възражения срещу сигнали за незаконно съдържание следва да е удобен за ползване и да предоставя възможност за подаване на възраженията по електронен път.
12. Следва да се гарантира, че доставчиците на хостинг услуги вземат надлежно предвид всички получени от тях възражения срещу сигнали за незаконно съдържание. Когато във възражението срещу сигнала за незаконно съдържание са посочени основания, поради които доставчикът на хостинг услуги счита, че съдържанието, за което се отнася възражението, не трябва да се счита за незаконно, той следва своевременно да оттегли решението си за премахване на това съдържание или за блокиране на достъпа до него, без да се засяга възможността на доставчика на хостинг услуги да определя условията си за ползване на услугата и да осигурява тяхното спазване в съответствие с правото на Съюза и правото на държавите членки.
13. Доставчикът на съдържание, който е подал възражение срещу сигнала за незаконно съдържание, и съответният подател на сигнал за незаконно съдържание следва, ако техните координати за връзка са известни на съответния доставчик на хостинг услуги, да бъдат информирани своевременно за решението на доставчика на хостинг услуги по отношение на съответното съдържание.

#### *Извънсъдебно уреждане на спорове*

14. Държавите членки се насърчават да подпомагат, когато е целесъобразно, извънсъдебното уреждане на споровете, свързани с премахване на незаконно съдържание или блокиране на достъпа до него. Механизмите за такова извънсъдебно уреждане на спорове следва да са лесно достъпни, ефективни, прозрачни и безпристрастни и да гарантират, че споразуменията са справедливи и спазват приложимото право. Опитите за извънсъдебно уреждане на такива спорове не следва да засягат достъпа на съответните страни до съд.
15. Доставчиците на хостинг услуги се насърчават да позволяват използването на извънсъдебни механизми за уреждане на спорове, когато такива механизми съществуват в съответната държава членка.

#### *Прозрачност*

16. Доставчиците на хостинг услуги следва да се насърчават да публикуват ясни, лесно разбираеми и достатъчно подробни обяснения на своята политика по отношение на премахването на съдържание или блокирането на достъпа до съдържание, което те съхраняват, включително съдържание, което те считат за незаконно.
17. Доставчиците на хостинг услуги следва да бъдат насърчавани да публикуват редовно, за предпочитане най-малко веднъж годишно, доклади относно своите дейности, свързани с премахването на съдържание, което се счита за незаконно, и блокирането на достъпа до такова съдържание. Тези доклади следва да включват по-специално информация относно количеството и вида на премахнатото съдържание, относно броя на получените сигнали за незаконно съдържание и на възраженията срещу такива сигнали и относно времето, необходимо за предприемане на действия.

*Проактивни мерки*

18. Доставчиците на хостинг услуги следва да се насърчават да предприемат, когато е целесъобразно, пропорционални и специфични проактивни мерки по отношение на незаконното съдържание. Такива проактивни мерки биха могли да включват използването на автоматизирани средства за откриване на незаконно съдържание само когато това е целесъобразно и пропорционално и са предвидени ефективни и подходящи гаранции, по-специално гаранциите, посочени в точки 19 и 20.

*Гаранции*

19. С цел да се избегне премахването на съдържание, което не е незаконно, и без да се засяга възможността доставчиците на хостинг услуги да определят условията си за ползване на услугата и да осигуряват спазването на тези условия в съответствие с правото на Съюза и правото на държавите членки, следва да съществуват ефективни и подходящи гаранции за надлежността и пропорционалността на действията на доставчиците на хостинг услуги по отношение на съдържанието, което съхраняват, по-специално при разглеждането на сигнали за незаконно съдържание и възражения срещу такива сигнали и при вземането на решение за евентуално премахване на съдържание, което се счита за незаконно, или за блокиране на достъпа до такова съдържание.
20. Когато доставчиците на хостинг услуги използват автоматизирани средства по отношение на съдържанието, което съхраняват, следва да бъдат осигурени ефективни и подходящи гаранции за точността и обосноваването на решенията, вземани във връзка със съдържанието, и по-специално на решенията за премахване на съдържание, което се счита за незаконно, или за блокирането на достъпа до такова съдържание. Тези гаранции следва по-специално да се изразяват в човешки контрол и проверки, когато това е целесъобразно и при всички случаи когато се изисква подробна преценка на съответния контекст, за да се определи дали съдържанието трябва да се счита за незаконно.

*Защита срещу злоупотреби*

21. Следва да се предприемат ефективни и подходящи мерки за предотвратяване на подаването на недобросъвестни сигнали за незаконно съдържание и на недобросъвестни възражения срещу сигнали за незаконно съдържание или за предотвратяване на предприемането на действия по такива сигнали и възражения, както и за предотвратяване на други злоупотреби, свързани с мерките за борба с незаконното съдържание онлайн, посочени в настоящата препоръка.

*Сътрудничество между доставчиците на хостинг услуги и държавите членки*

22. Държавите членки и доставчиците на хостинг услуги следва да определят звена за контакт по въпросите, свързани с незаконното съдържание онлайн.
23. Следва да бъдат предвидени ускорени процедури за разглеждане на сигнали за незаконно съдържание, подадени от компетентни органи.
24. Държавите членки се насърчават да установят правни задължения за доставчиците на хостинг услуги да информират незабавно правоприлагашите органи — за целите на предотвратяването, разследването, разкриването или наказателното преследване на престъпления — относно доказателства за предполагаеми тежки престъпления, свързани със заплаха за живота или безопасността на хора, получени в контекста на техните дейности по премахване на незаконно съдържание или блокиране на достъпа до такова съдържание, при спазване на приложимите правни изисквания, и по-специално на тези, свързани със защитата на личните данни, включително изискванията на Регламент (ЕС) 2016/679.

*Сътрудничество между доставчиците на хостинг услуги и доверените податели на сигнали за незаконно съдържание*

25. Сътрудничеството между доставчиците на хостинг услуги и доверените податели на сигнали за незаконно съдържание следва да се насърчава. Следва да бъдат предвидени по-специално ускорени процедури за разглеждане на сигнали за незаконно съдържание, подадени от доверени податели на такива сигнали.
26. Доставчиците на хостинг услуги следва да бъдат насърчавани да публикуват ясни и обективни условия за определяне на това кои физически лица или образувания те считат за доверени податели на сигнали за незаконно съдържание.
27. Тези условия следва да имат за цел да гарантират, че съответните физически лица или образувания притежават необходимите експертни познания и извършват надлежно и обективно дейностите си в качеството на доверени податели на сигнали за незаконно съдържание, зачитайки ценностите, на които се основава Съюзът.

*Сътрудничество между доставчиците на хостинг услуги*

28. Доставчиците на хостинг услуги следва да е целесъобразно, да споделят опит, технологични решения и най-добри практики в борбата с незаконното съдържание онлайн помежду си и по-специално с доставчиците на хостинг услуги, които поради своя размер или мащаба, в който работят, разполагат с ограничени ресурси и експертни познания, като това следва да се прави включително в контекста на текущото сътрудничество между доставчиците на хостинг услуги, осъществявано чрез кодекси за поведение, меморандуми за разбирателство и други доброволни договорености.

**ГЛАВА III****Специфични препоръки във връзка с терористичното съдържание***Общи положения*

29. Специфичните препоръки във връзка с терористичното съдържание, съдържащи се в настоящата глава, се прилагат в допълнение към общите препоръки, съдържащи се в глава II.
30. Доставчиците на хостинг услуги следва да посочват изрично в своите условия за ползване на услугата, че няма да съхраняват терористично съдържание.
31. Доставчиците на хостинг услуги следва да вземат мерки, що се отнася по-специално до сигналите за терористично съдържание, проактивните мерки и сътрудничеството в съответствие с точки 32—40, за да гарантират че не съхраняват терористично съдържание.

*Подаване и разглеждане на сигнали за терористично съдържание*

32. Държавите членки следва да гарантират, че техните компетентни органи имат капацитет и достатъчни ресурси за ефективно откриване и идентифициране на терористично съдържание, а така също и за подаване на сигнали за терористично съдържание до съответните доставчици на хостинг услуги, по-специално чрез националните звена за сигнализиране за терористично съдържание в интернет и в сътрудничество със звеното на ЕС за сигнализиране за терористично съдържание в интернет, което е част от Европол.
33. Следва да се предвидят разпоредби относно механизми, предоставящи възможност за подаване на сигнали за терористично съдържание. Следва да се предвидят ускорени процедури за разглеждане на сигналите за терористично съдържание, по-специално сигналите за терористично съдържание, подадени от националните звена за сигнализиране за терористично съдържание в интернет и от звеното на ЕС за сигнализиране за терористично съдържание в интернет към Европол.
34. Доставчиците на хостинг услуги следва своевременно да изпращат потвърждения за получаване на сигналите за терористично съдържание и да информират компетентния орган или Европол за решенията си във връзка със съдържанието, за което се отнасят сигналите, като според случая посочват момента, в който съдържанието е било премахнато или достъпът до него е бил блокиран, или причините, поради които са решили да не премахнат или блокират достъпа до съдържанието.
35. По правило доставчиците на хостинг услуги следва да преценят съдържанието, идентифицирано в сигнала за терористично съдържание, и при необходимост да го премахнат или блокират достъпа до него в рамките на един час от момента, в който са получили сигнала за терористично съдържание.

*Проактивни мерки*

36. Доставчиците на хостинг услуги следва да предприемат пропорционални и специфични проактивни мерки, включително чрез използване на автоматизирани средства, с цел откриване, идентифициране и експедитивно премахване на терористичното съдържание или блокиране на достъпа до него.
37. Доставчиците на хостинг услуги следва да предприемат пропорционални и специфични проактивни мерки, включително чрез използване на автоматизирани средства, за да попречат незабавно на доставчиците на съдържание да качат повторно съдържание, което вече е било премахнато или достъпът до което вече е бил блокиран, тъй като то се счита за терористично съдържание.

*Сътрудничество*

38. С цел да се предотврати разпространението на терористично съдържание в различни услуги за хостинг, доставчиците на хостинг услуги следва да бъдат насърчавани да си сътрудничат чрез обмен и оптимизиране на ефективни, подходящи и пропорционални технологични инструменти, включително такива инструменти, които позволяват автоматизирано откриване на съдържание. Когато е възможно от техническа гледна точка, следва да бъдат обхванати всички съответни формати, чрез които се разпространява терористично съдържание. Сътрудничеството следва да включва по-специално доставчиците на хостинг услуги, които поради своя размер или мащаба, в който работят, разполагат с ограничени ресурси и експертни познания.

39. Доставчиците на хостинг услуги следва да бъдат насърчавани да предприемат необходимите мерки за осигуряване на правилното функциониране и подобряването на инструментите, посочени в точка 38, по-специално чрез предоставяне на идентификатори, отнасящи се до цялото съдържание, което се счита за терористично, и чрез пълноценно използване на възможностите на тези инструменти.
40. Компетентните органи и доставчиците на хостинг услуги следва да сключват работни договорености, при необходимост и с Европол, по въпросите, свързани с терористичното съдържание онлайн, включително с цел повишаване на разбирането за терористичните дейности онлайн, подобряване на механизмите за сигнализиране за терористично съдържание, предотвратяване на ненужното дублиране на усилия и улесняване на исканията от правоприлагащите органи за целите на наказателните разследвания във връзка с тероризма.

#### ГЛАВА IV

##### Предоставяне на информация

41. Държавите членки следва да докладват на Комисията редовно и за предпочитане веднъж на всеки три месеца за сигналите за терористично съдържание, подадени от техните компетентни органи, и за решенията, взети от доставчиците на хостинг услуги по тези сигнали за терористично съдържание, както и за своето сътрудничество с доставчиците на хостинг услуги във връзка с борбата с терористичното съдържание.
42. За да дадат възможност за наблюдение на изпълнението на настоящата препоръка по отношение на терористичното съдържание не по-късно от три месеца от датата на нейното публикуване, доставчиците на хостинг услуги следва да предоставят на Комисията, по нейно искане, цялата необходима информация, позволяваща осъществяването на такова наблюдение. Тази информация може да включва по-специално информация за обема на съдържанието, което е било премахнато или достъпът до което е бил блокиран в отговор на сигнали за терористично съдържание или сигнали за незаконно съдържание или вследствие от проактивни мерки и използване на автоматизирани средства. Тя може също така да включва броя на получените сигнали за терористично съдържание и времето, необходимо за предприемане на действия, както и обема на съдържанието, чието подаване или повторно подаване е било предотвратено чрез използването на технологични инструменти за автоматизирано откриване на съдържание или други технологични инструменти.
43. За да дадат възможност за наблюдение на изпълнението на настоящата препоръка по отношение на незаконното съдържание, различно от терористично съдържание не по-късно от шест месеца от датата на нейното публикуване, доставчиците на хостинг услуги следва да предоставят на Комисията, по нейно искане, цялата необходима информация, позволяваща осъществяването на такова наблюдение.

Съставено в Брюксел на 1 март 2018 година.

За Комисията  
Andrus ANSIP  
Заместник-председател

---