Съвет на
Европейския съюз

Брюксел, 14 септември 2018 г.
(OR. en)

12129/18

Междуинституционално досие:
2018/0331 (COD)

CT 144
ENFOPOL 450
COTER 114
JAI 881
CYBER 193
TELECOM 288
FREMP 142
AUDIO 64
DROIPEN 127
COHOM 107
CODEC 1468

ПРЕДЛОЖЕНИЕ

От:	Генералния секретар на Европейската комисия, подписано от г-н Jordi AYET PUIGARNAU, директор
Дата на получаване:	12 септември 2018 г.
До:	Г-н Jeppe TRANHOLM-MIKKELSEN, генерален секретар на Съвета на Европейския съюз
№ док. Ком.:	COM(2018) 640 final
Относно:	Предложение за РЕГЛАМЕНТ НА ЕВРОПЕЙСКИЯ ПАРЛАМЕНТ И НА СЪВЕТА за предотвратяване на разпространението на терористично съдържание онлайн *Принос на Европейската комисия за срещата на лидерите в Залцбург на 19—20 септември 2018 г.*

Приложено се изпраща на делегациите документ COM(2018) 640 final.

Приложение: COM(2018) 640 final

ЕВРОПЕЙСКА
КОМИСИЯ

Брюксел, 12.9.2018 г.
COM(2018) 640 final

2018/0331 (COD)

Предложение за

РЕГЛАМЕНТ НА ЕВРОПЕЙСКИЯ ПАРЛАМЕНТ И НА СЪВЕТА

за предотвратяване на разпространението на терористично съдържание онлайн

Принос на Европейската комисия за срещата на лидерите в Залцбург на 19—20 септември 2018 г.

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

ОБЯСНИТЕЛЕН МЕМОРАНДУМ

1. КОНТЕКСТ НА ПРЕДЛОЖЕНИЕТО

1.1. Основания и цели на предложението

Повсеместността на интернет позволява на потребителите да комуникират, да работят, да общуват, да създават, получават и споделят информация и съдържание със стотици милиони хора по целия свят. Интернет платформите генерират значителни ползи за икономическото и социалното благосъстояние на потребителите в рамките на Съюза и извън него. Възможността обаче да се достигне до такава голяма аудитория при минимални разходи привлича също престъпници, които искат да злоупотребяват с интернет за незаконни цели. Неотдавнашните терористични нападения на територията на ЕС показаха как терористите злоупотребяват с интернет с цел да вербуват и набират поддръжници, да подготвят и улесняват терористична дейност, да възхваляват своите жестокости и да подтикват други да последват примера им, както и да всяват страх сред широката общественост.

Терористичното съдържание, споделяно онлайн за такива цели, се разпространява чрез доставчици на хостинг услуги, които позволяват качването на съдържание на трети страни. Доказана е важната роля на терористичното съдържание онлайн за радикализирането и за вдъхновяването на нападения от т.нар. „вълци единаци“ при няколко неотдавнашни терористични нападения в Европа. Това съдържание не само има значителни отрицателни последици за хората и за обществото като цяло, но също така намалява доверието на потребителите в интернет и засяга бизнес моделите и репутацията на засегнатите дружества. Терористи злоупотребяват не само с големите платформи на социалните медии, но и все повече с по-малки доставчици, които предлагат различни видове хостинг услуги в световен мащаб. При тази злоупотреба с интернет изпъкват особената обществена отговорност на интернет платформите за защита на потребителите от излагането им на терористично съдържание, както и сериозните рискове за сигурността, които това съдържание носи за обществото като цяло.

В отговор на призивите на публичните органи доставчиците на хостинг услуги въведоха някои мерки за борба с терористичното съдържание в своите услуги. Напредък бе постигнат чрез доброволни рамки и партньорства, включително интернет форума на ЕС, чието начало бе поставено през декември 2015 г. в рамките на Европейската програма за сигурност. Интернет форумът на ЕС насърчава доброволното сътрудничество между държавите членки и доставчиците на хостинг услуги и действията за намаляване на достъпността на терористичното съдържание онлайн и за предоставяне на възможности на гражданското общество да увеличи обема на ефективните алтернативни послания онлайн. Тези усилия допринесоха за засилване на сътрудничеството, подобряване на реакцията от страна на дружествата на сигналите от националните органи, както и от звеното на Европол за сигнализиране за незаконно съдържание в интернет, въвеждането на доброволни проактивни мерки за подобряване на автоматичното откриване на терористично съдържание, засиленото сътрудничество в рамките на сектора, включително разработването на „хеш-базата данни“ за предотвратяване на качването на известно терористично съдържание на свързани платформи, както и за повишената прозрачност на усилията. Макар че сътрудничеството в рамките на интернет форума на ЕС следва да продължи в бъдеще, доброволните договорености показаха и своите ограничения. На първо място, не всички засегнати доставчици на хостинг услуги участват във форума и на второ място,

мащабът и темпът на напредъка сред доставчиците на хостинг услуги като цяло не са достатъчни, за да се намери адекватен отговор на проблема.

Предвид тези ограничения е ясна необходимостта от засилени действия от страна на Европейския съюз срещу терористичното съдържание онлайн. На 1 март 2018 г. Комисията, като се опираше на съобщението на Комисията от септември[1], а също и на усилията в рамките на интернет форума на ЕС, прие препоръка относно мерки за ефективна борба с незаконното онлайн съдържание. В препоръката бе включена специална глава, в която се посочват поредица от мерки за ефективно предотвратяване на качването и споделянето онлайн на терористични пропагандни материали, като например подобрения в процеса на подаване на сигнали, едночасов срок, за да се реагира на сигналите, засилено проактивно откриване, ефективно премахване и достатъчни предпазни мерки за точна оценка на терористичното съдържание[2].

Необходимостта от засилване на действията във връзка с терористичното съдържание онлайн намери също така отражение в призиви на държавите — членки на ЕС, като някои от тях вече приеха законодателни актове или изразиха намерение за това. След поредица от терористични нападения в ЕС и предвид факта, че терористичното съдържание онлайн продължава да бъде лесно достъпно, Европейският съвет от 22 и 23 юни 2017 г. призова секторът да „разработи нови технологии и инструменти за подобряване на автоматичното откриване и премахване на съдържание, което подбужда към терористични актове. При необходимост това следва да бъде допълнено от съответни законодателни мерки на равнище ЕС“. Европейският съвет от 28 юни 2018 г. приветства „намерението на Комисията да представи законодателно предложение за подобряване на откриването и премахването на съдържание, което подбужда към омраза и към извършване на терористични актове“. Освен това Европейският парламент в своята резолюция относно онлайн платформите и цифровия единен пазар от 15 юни 2017 г. прикани настоятелно платформите „да засилят мерките за справяне с незаконното и вредното съдържание“, като същевременно призова Комисията да представи предложения за разрешаването на тези проблеми.

За да бъдат посрещнати тези предизвикателства и за да се отговори на призивите на държавите членки и на Европейския парламент, настоящото предложение на Комисията се стреми да установи ясна и хармонизирана правна рамка за предотвратяване на злоупотребата с хостинг услуги с цел разпространение на терористично съдържание онлайн, така че да се обезпечи гладкото функциониране на цифровия единен пазар, като същевременно се гарантират доверие и сигурност. Настоящият регламент има за цел да внесе яснота относно отговорността на доставчиците на хостинг услуги при предприемането на всички подходящи, разумни и пропорционални действия, необходими за гарантиране на безопасността на услугите им и за бързото и ефективно откриване и премахване на терористично съдържание онлайн, като се отчита фундаменталното значение на свободата на изразяване на мнение и на информация в едно отворено и демократично общество. С него се въвеждат също така поредица необходими гаранции, предназначени да гарантират пълното зачитане на основните права, като например свободата на изразяване на мнение и на информация в едно демократично общество, в допълнение към възможностите за съдебна защита,

[1] Съобщение (COM (2017) 555 final) относно борбата с незаконното онлайн съдържание.

[2] Препоръка (C(2018)1177 final) от 1 март 2018 г. относно мерки за ефективна борба с незаконното съдържание онлайн.

гарантирани чрез правото на ефективни правни средства за защита, предвидено в член 19 от ДЕС и член 47 от Хартата на основните права на ЕС.

Като определя минимален набор от задължения на доставчиците на хостинг услуги за полагането на грижи, в който са включени някои специфични правила и задължения, както и задължения на държавите членки, предложението има за цел да повиши ефективността на настоящите мерки за откриване, идентифициране и премахване на терористично съдържание онлайн, без това да засяга основни права, като например свободата на изразяване на мнение и свободата на информация. Тази хармонизирана правна рамка ще улесни предоставянето на онлайн услуги в рамките на цифровия единен пазар, ще осигури равни условия за всички доставчици на хостинг услуги, насочващи услугите си към Европейския съюз, и ще предостави стабилна правна уредба за откриването и премахването на терористично съдържание, придружена от съответни гаранции за защита на основните права. По-специално задълженията за прозрачност ще увеличат доверието сред гражданите, и по-специално ползвателите на интернет, и ще подобрят отчетността и прозрачността на действията на дружествата, включително по отношение на публичните органи. В предложението се определят също така задължения за въвеждане на правни средства за защита и механизми за подаване на жалби, за да се гарантира, че ползвателите могат да оспорят премахването на тяхното съдържание. Задълженията на държавите членки ще допринесат за постигането на тези цели, а също и за подобряване на способността на съответните органи да предприемат целесъобразни действия срещу терористичното съдържание онлайн и да се борят с престъпността. Когато доставчиците на хостинг услуги не спазват Регламента, държавите членки могат да налагат санкции.

1.2. Съгласуваност със съществуващата правна рамка на ЕС в тази област на политиката

Настоящото предложение е в съответствие с достиженията на правото на ЕС, свързани с цифровия единен пазар, и по-специално Директивата за електронната търговия. По-специално всички мерки, предприети от доставчика на хостинг услуги в съответствие с настоящия регламент, включително всички проактивни мерки, следва да не водят автоматично до невъзможност за съответния доставчик на услуги да се ползва от освобождаването от отговорност, предвидено при определени условия в член 14 от Директивата за електронната търговия. Решението на националните органи да налагат пропорционални и специфични проактивни мерки следва по принцип да не води до налагането на общо задължение за мониторинг, както е определено в член 15, параграф 1 от Директива 2000/31/ЕО по отношение на държавите членки. При все това, предвид особено сериозните рискове, свързани с разпространението на терористично съдържание, решенията съгласно настоящия регламент могат по изключение да предвидят дерогация от този принцип съгласно съответна уредба на ЕС. Преди приемането на тези решения компетентният орган следва да постигне справедлив баланс между нуждите, свързани с обществената сигурност, и засегнатите интереси и основни права, включително по-специално свободата на изразяване на мнение и свободата на информация, свободата на стопанска инициатива, защитата на личните данни и неприкосновеността на личния живот. Задълженията на доставчиците на хостинг услуги за полагане на грижи следва да отразяват и да зачитат този баланс, намерил израз в Директивата за електронната търговия.

Предложението е също така съгласувано и тясно свързано с Директива 2017/541/ЕС относно борбата с тероризма, чиято цел е да хармонизира законодателството на държавите членки, криминализиращо терористичните престъпления. Съгласно член 21

от Директивата за борба с тероризма от държавите членки се изисква да предприемат мерки, за да гарантират бързото премахване на онлайн съдържание, ограничено до публично подстрекаване, като изборът на мерките се оставя на държавите членки. С оглед на превантивния си характер настоящият регламент обхваща не само материали, подбуждащи към тероризъм, но също и материали за целите на набирането или обучението, което отразява други престъпления, свързани с терористични дейности, които също са предмет на Директива (ЕС) 2017/541. С настоящия регламент се налагат пряко задължения на доставчиците на хостинг услуги за полагането на грижи да премахват терористичното съдържание, както и се хармонизират процедурите за заповеди за премахване с цел да се намали достъпността на терористично съдържание онлайн.

С Регламента се допълват правилата, предвидени в бъдещата директива за аудио-визуалните медийни услуги, доколкото неговият персонален и материален обхват е по-широк. Регламентът обхваща не само платформите за споделяне на видеоматериали, но и всички различни видове доставчици на хостинг услуги. Освен това той обхваща не само видеозаписи, но и снимки и текст. И после настоящият регламент излиза извън обхвата на директивата по отношение на материалноправните разпоредби, като хармонизира правилата за искания за премахване на терористично съдържание, както и за проактивни мерки.

Предложеният регламент се основава на Препоръката на Комисията[3] относно незаконното съдържание от март 2018 г. Препоръката остава в сила, като всички, които имат роля за намаляване на достъпността на незаконно съдържание — включително терористично съдържание — следва да продължат да привеждат усилията си в съответствие с мерките, посочени в препоръката.

1.3. Кратко изложение на предложения регламент

Персоналният обхват на предложението включва доставчиците на хостинг услуги, които предлагат услугите си в рамките на Съюза, независимо от мястото им на установяване или размера им. С предложеното законодателство се въвеждат редица мерки за предотвратяване на злоупотребата с онлайн услуги за разпространение на терористично съдържание, за да се обезпечи гладкото функциониране на цифровия единен пазар, като същевременно се гарантират доверие и сигурност. Определението за незаконно терористично съдържание е в съответствие с определението за терористични престъпления, посочено в Директива (ЕС) 2017/541, и обхваща информация, която се използва за подбуждане към и възхваляване на извършването на терористични престъпления, като се насърчава съучастието и се предоставят указания за извършване на терористични престъпления, както и се популяризира участието в терористични групи.

За да се гарантира премахването на незаконно терористично съдържание, с Регламента се въвежда заповед за премахване, която може да бъде издадена като административно или съдебно решение от компетентен орган в държава членка. В тези случаи доставчикът на хостинг услуги е длъжен да премахне съдържанието или да блокира достъпа до него в рамките на един час. Освен това Регламентът хармонизира минималните изисквания за сигнали, изпращани за оценка от компетентните органи на държавите членки и от органите на Съюза (като например Европол) до доставчиците на

[3] Препоръка (C(2018)1177 final) от 1 март 2018 г. относно мерки за ефективна борба с незаконното съдържание онлайн.

хостинг услуги при спазване на съответните им условия. И накрая, в Регламента се изисква доставчиците на хостинг услуги да предприемат, когато е целесъобразно, проактивни мерки, пропорционални на равнището на риска, и да премахват терористични материали от своите услуги, включително чрез внедряване на автоматизирани инструменти за откриване.

Мерките, насочени към намаляване на терористичното съдържание онлайн, са придружени от редица ключови гаранции, за да се гарантира пълната защита на основните права. Като част от мерките за защита на съдържание, което не е терористично съдържание, от погрешно премахване, в предложението се определят задължения за създаване на правни средства за защита и механизми за подаване на жалби, за да се гарантира, че ползвателите могат да оспорят премахването на съдържанието им. Освен това с Регламента се въвеждат задължения за прозрачност по отношение на мерките, предприети срещу терористично съдържание от доставчиците на хостинг услуги, като по този начин се гарантира отчетност спрямо ползвателите, гражданите и публичните органи.

Регламентът задължава също така държавите членки да гарантират, че техните компетентни органи разполагат с необходимия капацитет за намеса срещу терористично съдържание онлайн. В допълнение държавите членки са задължени да се информират и да си сътрудничат помежду си и могат да използват каналите, създадени от Европол, за да осигурят координация по отношение на заповеди за премахване и сигнали. В Регламента се предвиждат също така задължения за доставчиците на хостинг услуги да докладват по-подробно за предприетите мерки и да информират правоприлагащите органи, когато откриват съдържание, което представлява заплаха за живота или безопасността. На последно място, съществува задължение за доставчиците на хостинг услуги да запазват съдържанието, което премахват, което действа като предпазна мярка срещу погрешно премахване и гарантира, че няма да бъдат загубени потенциални доказателства за целите на предотвратяването, разкриването, разследването и наказателното преследване на терористични престъпления.

2. ПРАВНО ОСНОВАНИЕ, СУБСИДИАРНОСТ И ПРОПОРЦИОНАЛНОСТ

2.1. Правно основание

Правното основание е член 114 от Договора за функционирането на Европейския съюз, в който се предвижда въвеждането на мерки, които да гарантират функционирането на вътрешния пазар.

Член 114 е подходящото правно основание за хармонизиране на условията за доставчиците на хостинг услуги при предоставянето на трансгранични услуги в рамките на цифровия единен пазар и за преодоляване на различията между разпоредбите на държавите членки, които в противен случай биха могли да възпрепятстват функционирането на вътрешния пазар. Той също така предотвратява появата на бъдещи пречки пред икономическата дейност, дължащи се на различия в начина, по който би могло да се развива националното законодателство.

Член 114 от ДФЕС може да се използва и за налагане на задължения на доставчици на услуги, установени извън територията на ЕС, когато предоставянето на услуги засяга вътрешния пазар, тъй като това е необходимо за постигането на желаната цел на вътрешния пазар.

2.2. Избор на инструмент

С член 114 от ДФЕС на законодателя на Съюза се дава възможността да приема регламенти и директиви.

Тъй като предложението се отнася до задължения на доставчиците на услуги, които обикновено предлагат услугите си в повече от една държава членка, различията в прилагането на тези правила биха попречили на предоставянето на услуги от доставчици, работещи в няколко държави членки. Регламентът дава възможност едно задължение да се наложи по еднакъв начин в Съюза, е пряко приложим, осигурява яснота и по-голяма правна сигурност и избягва различното транспониране в държавите членки. По тези причини се счита, че най-подходящата форма, която да бъде използвана за този инструмент, е регламентът.

2.3. Субсидиарност

Като се има предвид трансграничното измерение на разглежданите проблеми, за да се постигнат целите, мерките, включени в предложението, трябва да бъдат приети на равнището на Съюза. По своето естество интернет е трансграничен и по принцип достъп до съдържание, хоствано в една държава членка, е възможен от всяка друга държава членка.

Започва да се оформя разпокъсана уредба от национални правила за противодействие на терористично съдържание онлайн и рисковете се увеличават. Това би довело до тежест за дружествата във връзка със спазването на различните разпоредби и до създаването на неравни условия за дружествата, а също и до „вратички в областта на сигурността“.

Поради това евентуално действие на ЕС повишава правната сигурност и увеличава ефективността на действията на доставчиците на хостинг услуги срещу терористичното съдържание онлайн. Това следва да даде възможност на повече дружества да предприемат действия, включително на дружества, установени извън Европейския съюз, така че да се укрепи целостта на цифровия единен пазар.

Това оправдава необходимостта от действие на ЕС, както се потвърждава в заключенията на Европейския съвет от юни 2018 г., в които Комисията се приканва да представи законодателно предложение в тази област.

2.4. Пропорционалност

В предложението се определят правила за доставчиците на хостинг услуги във връзка с прилагането на мерки за експедитивно премахване на терористично съдържание от техните услуги. Основните елементи ограничават предложението само до това, което е необходимо за постигане на целите на политиката.

В предложението се вземат предвид тежестта за доставчиците на хостинг услуги и гаранциите, включително защитата на свободата на изразяване на мнение и свободата на информация, както и други основни права. Едночасовият срок за премахване се прилага само за заповедите за премахване, издадени въз основа на решение, подлежащо на съдебен контрол, с което компетентните органи са установили незаконността. Що се отнася до сигналите, съществува задължение за въвеждането на мерки за улесняване на експедитивната оценка на терористичното съдържание, без обаче да се налагат задължения за премахването му, нито абсолютни срокове за това. Окончателното решение остава да бъде доброволно взето от доставчика на хостинг услуги. Тежестта за дружествата да оценяват съдържанието е облекчена от факта, че компетентните органи

на държавите членки и органите на Съюза предоставят обяснения защо съдържанието може да се счита за терористично съдържание. Когато е целесъобразно, доставчиците на хостинг услуги предприемат проактивни мерки, за да предпазят своите услуги от разпространението на терористично съдържание. Специфичните задължения, свързани с проактивни мерки, са ограничени до доставчиците на хостинг услуги, които са изложени на терористично съдържание, както е видно от получаването на заповед за премахване, която е станала окончателна, и следва да бъдат пропорционални както на степента на риска, така и на ресурсите на дружеството. Запазването на премахнатото съдържание и свързаните с него данни е ограничено до срок, който е пропорционален с оглед на предоставянето на възможност за процедури за административен или съдебен контрол и за предотвратяването, разкриването, разследването и наказателното преследване на терористични престъпления.

3. РЕЗУЛТАТИ ОТ ПОСЛЕДВАЩИТЕ ОЦЕНКИ, ОТ КОНСУЛТАЦИИТЕ СЪС ЗАИНТЕРЕСОВАНИТЕ СТРАНИ И ОТ ОЦЕНКИТЕ НА ВЪЗДЕЙСТВИЕТО

3.1. Консултации със заинтересованите страни

При изготвянето на настоящото законодателно предложение Комисията се консултира с всички съответни заинтересовани страни, за да разбере техните гледища и възможните следващи стъпки. Комисията проведе открита обществена консултация относно мерките за подобряване на ефективността на борбата с незаконното съдържание, като получи 8 961 отговора, от които 8 749 бяха от физически лица, 172 — от организации, 10 — от публични администрации, както и 30 от други категории анкетирани. Успоредно с това беше проведено проучване на Евробарометър със случайна извадка от 33 500 пребиваващи в ЕС лица относно незаконното съдържание онлайн. Комисията също така се консултира през май и юни 2018 г. с органите на държавите членки, както и с доставчиците на хостинг услуги по отношение на специфични мерки за борба с терористичното съдържание онлайн.

Като цяло мнозинството заинтересовани страни изразиха мнението, че терористичното съдържание онлайн е сериозен социален проблем, който засяга ползвателите на интернет и бизнес моделите на доставчиците на хостинг услуги. В по-общ план 65 % от анкетираните в проучването на Евробарометър[4] считат, че интернет не е безопасен за потребителите, а 90 % от анкетираните смятат, че е важно да се ограничи разпространението на незаконно съдържание онлайн. Консултациите с държавите членки показаха, че макар доброволните споразумения да водят до резултати, много от държавите виждат необходимост от обвързващи задължения по отношение на терористичното съдържание — нагласа, отразена в заключенията на Европейския съвет от юни 2018 г. Макар че доставчиците на хостинг услуги като цяло подкрепиха продължаването на доброволните мерки, те отбелязаха потенциалните отрицателни ефекти от оформящата се правна разпокъсаност в Съюза.

Много от заинтересованите страни също така отбелязаха необходимостта да се гарантира, че всички регулаторни мерки за премахване на съдържание, особено проактивните мерки и стриктните срокове, следва да бъдат балансирани с гаранции за основните права, и по-специално свободата на изразяване на мнение. Заинтересованите страни отбелязаха редица необходими мерки, свързани с прозрачността, отчетността,

[4] Евробарометър 469, „Незаконно съдържание онлайн“, юни 2018 г.

както и необходимостта от механизми за преглед от хора при внедряването на автоматизирани инструменти.

3.2. Оценка на въздействието

Комитетът за регулаторен контрол даде положително становище с резерви относно оценката на въздействието и направи различни предложения за подобрение[5]. След това становище докладът за оценка на въздействието беше изменен, за да бъдат взети предвид основните коментари на Съвета, като се постави акцент конкретно върху терористичното съдържание и същевременно допълнително се набляга на последиците за функционирането на цифровия единен пазар и се анализират по-задълбочено въздействието върху основните права и функционирането на предпазните мерки, предложени във вариантите.

Ако не бъдеха предприети допълнителни мерки, можеше да се очаква, че доброволните действия съгласно базовия сценарий ще продължат, като имат известно въздействие за намаляването на терористичното съдържание онлайн. Малко вероятно бе обаче, че всички доставчици на хостинг услуги, изложени на такова съдържание, биха предприели доброволни мерки, като се очакваше появата на допълнително разпокъсване, водещо до допълнителни бариери пред трансграничното предоставяне на услуги. Редом с базовия сценарий бяха разгледани три основни варианта на политиката с нарастваща степен на ефективност по отношение на целите, посочени в оценката на въздействието, и общата цел на политиката за намаляване на терористичното съдържание онлайн.

И в трите варианта обхватът на тези задължения бе насочен към всички доставчици на хостинг услуги (персонален обхват), установени в ЕС и в трети държави — доколкото предлагат услугите си в Съюза (географски обхват). Предвид естеството на проблема и необходимостта да не се допуска злоупотребата с по-малките платформи в нито един от вариантите не бяха предвидени изключения за МСП. При всички варианти е налице изискване към доставчиците на хостинг услуги за определянето на законен представител в ЕС, включително за дружества, установени извън ЕС, така че да бъде гарантирано изпълнението на правилата на ЕС. Съгласно всички варианти се предвижда разработването от страна на държавите членки на механизми за санкции.

Всички варианти предвиждат създаването на нова, хармонизирана система на законови заповеди за премахване на терористично съдържание онлайн, издадени на доставчиците на хостинг услуги от националните органи, и изискването за премахване на това съдържание в едночасов срок. Тези заповеди не биха съдържали задължение за оценка от страна на доставчиците на хостинг услуги и би трябвало да подлежат на обжалване.

Предпазните мерки, по-специално процедурите за подаване на жалби и ефективните правни средства за защита, включително съдебна защита, както и други разпоредби за предотвратяване на погрешното премахване на съдържание, което не е терористично съдържание, като същевременно се гарантира зачитането на основни права, са общи елементи на трите варианта. Освен това всички варианти включват задължения за докладване под формата на публична прозрачност и на докладване на държавите членки и на Комисията, както и на органите при подозрение за извършено престъпление. В допълнение се предвиждат задължения за сътрудничество между

[5] Връзка към становището на Комитета за регулаторен контрол на RegDoc.

националните органи, доставчиците на хостинг услуги и когато е целесъобразно, Европол.

Основните разлики между трите варианта са свързани с обхвата на определението за терористично съдържание, равнището на хармонизация на сигналите, обхвата на проактивните мерки, задълженията за координация на държавите членки, както и изискванията за съхраняване на данни. Вариант 1, следвайки тясно определение, би ограничил обхвата на материалите до съдържание, разпространявано с цел пряко подбуждане към извършване на терористичен акт, докато при варианти 2 и 3 би се възприел по-всеобхватен подход, обхващащ и материали за набиране и обучение. По отношение на проактивните мерки при вариант 1 доставчиците на хостинг услуги, изложени на терористично съдържание, ще трябва да извършат оценка на риска, но проактивните мерки по отношение на риска остават на доброволни начала. При вариант 2 се изисква доставчиците на хостинг услуги да изготвят план за действие, който може да включва внедряването на автоматизирани инструменти за предотвратяване на повторно качване на вече премахнато съдържание. Вариант 3 включва по-всеобхватни проактивни мерки, изискващи от доставчиците на услуги, изложени на терористично съдържание, да идентифицират и новите материали. При всички варианти изискванията, свързани с проактивни мерки, ще бъдат пропорционални на равнището на експозиция на терористични материали, както и на икономическия капацитет на доставчика на услуги. Що се отнася до сигналите, вариант 1 не би хармонизирал подхода към сигналите, докато вариант 2 би направил това по отношение на Европол, а вариант 3 би включил и сигнали от държавите членки. При варианти 2 и 3 държавите членки ще бъдат задължени да се информират, да се координират и да си сътрудничат помежду си, а при вариант 3 те ще трябва също да гарантират, че техните компетентни органи разполагат с капацитет да откриват и да уведомяват за терористично съдържание. И накрая, вариант 3 включва също изискване за съхраняване на данните като предпазна мярка в случаи на погрешно премахване, както и за улесняване на наказателните разследвания.

В допълнение към правните разпоредби бе предвидено всички законодателни варианти да бъдат придружени от редица подкрепящи мерки, по-специално способстващи за сътрудничеството между националните органи и Европол, както и сътрудничеството с доставчиците на хостинг услуги, и за подкрепата за научните изследвания, развойните дейности и иновациите с цел разработване и внедряване на технологични решения. След приемането на правния инструмент може да бъдат използвани и допълнителни инструменти за повишаване на осведомеността и подкрепа на МСП.

В оценката на въздействието се стигна до заключението, че са необходими редица мерки за постигане на целта на политиката. Всеобхватното определение на терористичното съдържание, включващо най-вредните материали, е за предпочитане пред тясно определение на съдържанието (вариант 1). Проактивните задължения, ограничени до предотвратяването на повторно качване на терористично съдържание (вариант 2), биха имали по-слабо въздействие в сравнение със задължения, свързани с откриването на терористично съдържание (вариант 3). Разпоредбите относно сигналите следва да включват сигнали като от Европол, така и от държавите членки (вариант 3) и да не бъдат ограничавани само до сигнали от Европол (вариант 2), тъй като сигналите от държавите членки са важен принос като част от общото усилие за намаляване на достъпността на терористичното съдържание онлайн. Необходимо би било тези мерки да бъдат изпълнени в допълнение към мерките, които са общи за всички варианти,

включително солидните предпазни мерки срещу погрешното премахване на съдържание.

3.3. Основни права

Онлайн пропагандата на терористите се стреми да подстрекава хората да извършват терористични нападения, включително като ги снабдява с подробни указания относно начините за нанасяне на максимални вреди. Тези зверства обикновено са последвани от допълнителна пропаганда, чрез която терористите възхваляват своите актове и насърчават други да последват примера им. Настоящият регламент допринася за защитата на обществената сигурност чрез намаляване на достъпността на терористично съдържание, което подбужда към и насърчава нарушаването на основни права.

Предложението би могло евентуално да засегне редица основни права:

а) правата на доставчиците на съдържание: правото на свобода на изразяване на мнение; правото на защита на личните данни; правото на зачитане на личния и семейния живот, принципа на недискриминация и правото на ефективни правни средства за защита;

б) правата на доставчиците на услуги: правото на свобода на стопанската инициатива; правото на ефективни правни средства за защита;

в) правата на всички граждани и правото на свобода на изразяване на мнение и свобода на информация.

Като отчита съответните достижения на правото на ЕС, предлаганият регламент включва достатъчни и солидни гаранции, които да гарантират защитата на правата на тези лица.

Първият елемент в този контекст е, че с Регламента се установява определение за терористично съдържание онлайн в съответствие с определението за терористични престъпления в Директива (ЕС) 2017/541. Това определение се прилага за заповеди за премахване и сигнали, а също и за проактивни мерки. Определението гарантира, че се премахва единствено незаконното съдържание, което съответства на валидно в целия Съюз определение на съответните престъпления. Освен това Регламентът включва общи задължения за полагане на грижа от страна на доставчиците на хостинг услуги, така че да действат по старателен, пропорционален и недискриминационен начин по отношение на съдържанието, което съхраняват, по-специално когато прилагат своите условия за ползване, за да се избегне премахването на съдържание, което не е терористично.

По-конкретно Регламентът е замислен така, че да се гарантира пропорционалност на мерките, предприети по отношение на основните права. Що се отнася до заповедите за премахване, оценката на съдържанието (включително правните проверки, когато е необходимо) от страна на компетентния орган обосновава срока от един час за премахване при тази мярка. Освен това разпоредбите в настоящия регламент, отнасящи се до сигнали, се ограничават до сигналите, изпратени от компетентните органи и органите на Съюза, в които се дава обяснение защо съдържанието може да се счита за терористично съдържание. При все че доставчикът на хостинг услуги отговаря за премахването на съдържанието, посочено в сигнала, това решение се улеснява от горепосочената оценка.

При проактивните мерки отговорността за идентифициране, оценяване и премахване на съдържание продължава да се носи от доставчиците на хостинг услуги, като от тях се изисква да въведат предпазни мерки, за да се гарантира, че съдържанието не се отстранява погрешно, включително чрез преглед от хора, особено ако е необходимо допълнително поставяне в контекст. Освен това, за разлика от основния сценарий, при който най-засегнатите дружества създават автоматизирани инструменти без публичен надзор, планираните мерки и тяхното прилагане ще бъдат предмет на докладване пред компетентните органи в държавите членки. Това задължение намалява риска от погрешни премахвания както за дружества, които създават нови инструменти, така и за тези, които вече ги използват. В допълнение от доставчиците на хостинг услуги се изисква да осигурят на доставчиците на съдържание лесни за ползване механизми за подаване на жалби, с които да оспорват решението за премахване на съдържанието им, както и да публикуват доклади за прозрачност за широката общественост.

И накрая, в случай че независимо от тези предпазни мерки, съдържанието и свързаните с него данни бъдат погрешно премахнати, от доставчиците на хостинг услуги се изисква да ги запазят за срок от шест месеца, така че да могат да ги възстановят, за да се гарантира ефективността на процедурите за подаване на жалби и за тяхното разглеждане с цел защита на свободата на изразяване на мнение и свободата на информация. В същото време запазването допринася и за целите на правоприлагането. Доставчиците на хостинг услуги трябва да въведат технически и организационни предпазни мерки, за да се гарантира, че данните не се използват за други цели.

Предложените мерки, по-специално свързаните със заповеди за премахване, сигнали, проактивни мерки и съхраняването на данни, следва не само да защитават ползвателите на интернет срещу терористично съдържание, но и да допринасят за защитата на правото на живот на гражданите чрез намаляване на достъпността на терористично съдържание онлайн.

4. ОТРАЖЕНИЕ ВЪРХУ БЮДЖЕТА

Законодателното предложение за регламент не дава отражение върху бюджета на Съюза.

5. ДРУГИ ЕЛЕМЕНТИ

5.1. Планове за изпълнение и механизми за мониторинг, оценка и докладване

Комисията ще изготви в срок от [една година от датата на прилагане на настоящия регламент] подробна програма за мониторинг на крайните продукти, резултатите и въздействието на настоящия регламент. В програмата за мониторинг се определят показателите и средствата, чрез които се събират данните и другите необходими доказателства, и на какви интервали ще става това. В нея се посочват действията, които да бъдат предприети от Комисията и от държавите членки при събирането и анализирането на данните и другите доказателства с оглед на мониторинга на напредъка и на оценката на настоящия регламент.

Въз основа на установената програма за мониторинг в рамките на две години от влизането в сила на настоящия регламент Комисията ще докладва за прилагането на настоящия регламент въз основа на докладите за прозрачност, публикувани от дружествата, както и на информацията, предоставена от държавите членки. Комисията ще извърши оценка не по-рано от четири години след влизането в сила на Регламента.

Въз основа на констатациите в оценката, включително това дали са останали пропуски или слабости, които имат значение на практика, и като се има предвид технологичното развитие, Комисията ще направи оценка на необходимостта от разширяване на приложното поле на Регламента. Ако е необходимо, Комисията ще представи предложения за адаптиране на настоящия регламент.

Комисията ще подпомага изпълнението, мониторинга и оценката на Регламента чрез експертна група на Комисията. Групата ще способства също така за сътрудничеството между доставчиците на хостинг услуги, правоприлагащите органи и Европол; ще насърчава обмена и практиките за откриване и премахване на терористично съдържание, ще предоставя своя експертен опит относно развитието на начина на действие на терористите в интернет; както и ще предоставя съвети и насоки, когато е уместно, за да се даде възможност за прилагане на разпоредбите.

Прилагането на предложения регламент може да бъде улеснено чрез редица подкрепящи мерки. Те включват евентуалното разработване на платформа в рамките на Европол за подпомагане на координирането на сигналите и заповедите за премахване. Финансираните от ЕС научни изследвания относно развитието на начина на действие на терористите подобряват разбирането и осведомеността на всички заинтересовани страни. Освен това в рамките на „Хоризонт 2020“ се подпомагат научни изследвания с цел разработване на нови технологии, включително автоматизирано предотвратяване на качването на терористично съдържание. В допълнение Комисията ще продължи да анализира начините за подпомагане на компетентните органи и доставчиците на хостинг услуги при прилагането на настоящия регламент посредством финансовите инструменти на ЕС.

5.2. Подробно разяснение на отделните разпоредби на предложението

В член 1 се определя предметът, като се посочва, че с Регламента се установяват правила за предотвратяване на злоупотребата с хостинг услуги за разпространение на терористично съдържание онлайн, включително по отношение на задълженията за полагане на грижи на доставчиците на хостинг услуги, както и на мерките, които държавите членки трябва да въведат. В него също така се определя географският обхват, обхващащ доставчиците на хостинг услуги, които предлагат услуги в Съюза, независимо от мястото им на стопанска дейност.

В член 2 се съдържат определенията на понятията, използвани в предложението. В него се съдържа и определение за терористично съдържание с превантивна цел въз основа на Директивата относно борбата с тероризма, така че да включва материали и информация, които подбуждат, насърчават или пропагандират извършването на терористични престъпления или на съучастието в тях, предоставят указания за извършването на такива престъпления или популяризират участието в дейности на терористична група.

В член 3 се предвиждат задължения за полагане на грижи, които да се прилагат от доставчиците на хостинг услуги при предприемане на действия в съответствие с настоящия регламент, и по-специално при надлежно зачитане на съответните основни права. В него се предвиждат подходящи разпоредби, които да бъдат въведени в рамките на условията за ползване на доставчиците на хостинг услуги, като след това се гарантира, че те се прилагат.

С член 4 от държавите членки се изисква да оправомощят компетентните органи да издават заповеди за премахване и се предвижда изискване към доставчиците на хостинг услуги да премахват съдържанието в срок от един час от получаването на заповедта за премахване. В него се определят също така минималните елементи, които заповедите за премахване следва да съдържат, и процедурите за доставчиците на хостинг услуги, с които да предоставят обратна информация на издаващия орган, както и да го информират, ако не е възможно да се изпълни заповедта или ако са необходими допълнителни пояснения. В него също така се изисква издаващият орган да информира органа, който наблюдава проактивните мерки на държавата членка, под чиято юрисдикция е доставчикът на хостинг услуги.

В член 5 се определя изискване към доставчиците на хостинг услуги да въведат мерки за експедитивно оценяване на съдържание, сигнализирано чрез сигнал от компетентен орган в държава членка или орган на Съюза, без обаче да е наложено изискване за премахване на сигнализираното съдържание, нито са определени конкретни срокове за предприемане на действие. В него се определят също така минималните елементи, които сигналите следва да съдържат, и процедурите за доставчиците на хостинг услуги, с които да предоставят обратна информация на издаващия орган или да поискат пояснения от органа, сигнализирал за съдържанието.

В член 6 от доставчиците на хостинг услуги се изисква да предприемат ефективни и пропорционални проактивни мерки, когато е целесъобразно. В него се установява процедура, която гарантира, че някои доставчици на хостинг услуги (т.е. тези, получили заповед за премахване, която е станала окончателна) предприемат допълнителни проактивни мерки, когато е необходимо, за да се намалят рисковете и в съответствие с излагането на терористично съдържание в техните услуги. Доставчикът на хостинг услуги следва да сътрудничи на компетентния орган по отношение на необходимите мерки, които се изискват, и ако не може да бъде постигнато споразумение, органът може да наложи мерки на доставчика на услуги. В този член се установява също така процедура за обжалване на решението на органа.

В член 7 от доставчиците на хостинг услуги се изисква да съхраняват премахнатото съдържание и свързаните с него данни за срок от шест месеца във връзка с процедурите за обжалване и за целите на разследването. Този срок може да бъде удължен, за да се даде възможност за приключване на обжалването. В този член се изисква също така доставчиците на услуги да въведат предпазни мерки, за да се гарантира, че не се предоставя достъп до съхраняваното съдържание и свързаните с него данни, както и че те не се обработват за други цели.

В член 8 се установява задължение за доставчиците на хостинг услуги да обясняват своите политики срещу терористично съдържание и да публикуват годишни доклади за прозрачността относно действията, предприети в това отношение.

В член 9 са предвидени специални гаранции по отношение на използването и прилагането на проактивни мерки при използването на автоматизирани средства, за да се гарантира, че решенията са точни и добре обосновани.

В член 10 от доставчиците на хостинг услуги се изисква да прилагат механизми за подаване на жалби по отношение на премахване, сигнали и проактивни мерки, както и да разглеждат своевременно всяка жалба.

В член 11 се установява задължение за доставчиците на хостинг услуги да предоставят на доставчика на съдържанието информация относно премахването му освен ако компетентният орган изисква неоповестяването от съображения за обществена сигурност.

Член 12 изисква от държавите членки да гарантират, че компетентните органи разполагат с достатъчни капацитет и ресурси, за да изпълняват своите задължения съгласно настоящия регламент.

В член 13 от държавите членки се изисква да сътрудничат помежду си и когато е необходимо, с Европол, за да се избегне дублирането и намесата в разследванията. В този член се предвижда също възможността за държавите членки и доставчиците на хостинг услуги да използват специални инструменти, включително тези на Европол, за обработването и обратната информация, свързани със заповеди за премахване и сигнали, както и да си сътрудничат по отношение на проактивни мерки. В него също така се изисква държавите членки да разполагат с подходящи канали за комуникация, за да се гарантира своевременен обмен на информация при изпълнението и прилагането на разпоредбите на настоящия регламент. Този член задължава също така доставчиците на хостинг услуги да информират съответните органи, когато узнаят за доказателства за терористични престъпления по смисъла на член 3 от Директива (ЕС) 2017/541 относно борбата с тероризма.

В член 14 се предвижда създаването на звена за контакт както от доставчиците на хостинг услуги, така и от държавите членки, за да се улесни комуникацията между тях, по-специално във връзка със заповеди за премахване и сигнали.

С член 15 се установява юрисдикцията на държавата членка за целите на надзора върху проактивните мерки, определянето на санкции и усилията за мониторинг.

В член 16 се изисква от доставчиците на хостинг услуги, които нямат място на стопанска дейност в държава членка, но предлагат услуги в рамките на Съюза, да определят законен представител в Съюза.

В член 17 от държавите членки се изисква да определят органи за издаването на заповеди за премахване, за сигнализирането на терористично съдържание, за наблюдението на прилагането на проактивни мерки и за прилагането на Регламента.

В член 18 се посочва, че държавите членки следва да установят правила относно санкциите при неспазване, и се предвиждат критерии, които държавите членки трябва да вземат предвид при определянето на вида и размера на санкциите. Като се има предвид особеното значение на експедитивното премахване на терористично съдържание, идентифицирано в заповед за премахване, следва да се въведат конкретни правила относно финансовите санкции за системни нарушения на това изискване.

В член 19 се установява по-бърза и по-гъвкава процедура за изменение на образците, предоставени за заповедите за премахване, и на каналите за подаване с удостоверена автентичност чрез делегирани актове.

В член 20 се определят условията, при които Комисията има правомощието да приема делегирани актове, за да се предвидят необходимите изменения на образците и техническите изисквания за заповедите за премахване.

С член 21 от държавите членки се изисква да събират и докладват специфична информация, свързана с прилагането на Регламента, с цел да съдействат на Комисията при изпълнението на нейните задължения по член 23. Комисията изготвя подробна програма за мониторинг на крайните продукти, резултатите и въздействието на настоящия регламент.

В член 22 се посочва, че Комисията ще докладва за прилагането на настоящия регламент две години след влизането му в сила.

В член 23 се посочва, че Комисията ще докладва за оценката на настоящия регламент три години след влизането му в сила.

В член 24 се постановява, че предложеният регламент ще влезе в сила на двадесетия ден след деня на публикуването му в *Официален вестник* и след това ще започне да се прилага 6 месеца след датата на влизането му в сила. Този срок се предлага с оглед на необходимостта от мерки за прилагане, като същевременно се признава спешната необходимост от цялостно прилагане на правилата на предложения регламент. Този краен срок от 6 месеца е определен въз основа на предположението, че преговорите ще бъдат проведени бързо.

2018/0331 (COD)

Предложение за

РЕГЛАМЕНТ НА ЕВРОПЕЙСКИЯ ПАРЛАМЕНТ И НА СЪВЕТА

за предотвратяване на разпространението на терористично съдържание онлайн

Принос на Европейската комисия за срещата на лидерите в Залцбург на 19—20 септември 2018 г.

ЕВРОПЕЙСКИЯТ ПАРЛАМЕНТ И СЪВЕТЪТ НА ЕВРОПЕЙСКИЯ СЪЮЗ,

като взеха предвид Договора за функционирането на Европейския съюз, и по-специално член 114 от него,

като взеха предвид предложението на Европейската комисия,

след предаване на проекта на законодателния акт на националните парламенти,

като взеха предвид становището на Европейския икономически и социален комитет[6],

в съответствие с обикновената законодателна процедура,

като имат предвид, че:

(1) Настоящият регламент има за цел да гарантира безпрепятственото функциониране на цифровия единен пазар в едно отворено и демократично общество, като се предотвратява злоупотребата с хостинг услуги за терористични цели. Функционирането на цифровия единен пазар следва да бъде подобрено чрез засилване на правната сигурност за доставчиците на хостинг услуги, укрепване на доверието на ползвателите в онлайн средата и засилване на гаранциите за свободата на изразяване на мнение и свободата на информация.

(2) Доставчиците на хостинг услуги, осъществяващи дейност чрез интернет, играят съществена роля в цифровата икономика, като свързват бизнеса и гражданите и улесняват обществения дебат и разпространението и получаването на информация, мнения и идеи, допринасяйки в значителна степен за иновациите, икономическия растеж и създаването на работни места в Съюза. В някои случаи обаче техните услуги стават обект на злоупотреби от страна на трети лица с цел извършване на незаконни дейности онлайн. Повод за особено безпокойство буди злоупотребата с доставчици на хостинг услуги от страна на терористични групи и на техните поддръжници, за да разпространяват терористично съдържание онлайн с цел отправяне на послания, радикализиране и вербуване, както и улесняване и ръководене на терористична дейност.

[6] ОВ C [...], [...] г., стр. [...].

(3) Наличието на терористично съдържание онлайн има сериозни отрицателни последици за ползвателите, гражданите и обществото като цяло, както и за доставчиците на онлайн услуги, които хостват такова съдържание, тъй като то подкопава доверието на техните ползватели и вреди на бизнес моделите им. 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 защитават своите услуги срещу злоупотреба от терористи и да помагат борбата с терористичното съдържание, разпространявано чрез използването на техните услуги.

(4) Усилията на равнището на Съюза за борба с терористично съдържане онлайн, които започнаха през 2015 г. чрез рамка за доброволно сътрудничество между държавите членки и доставчиците на хостинг услуги, трябва да бъдат допълнени с ясна законодателна рамка с цел допълнително ограничаване на достъпността на терористично съдържание онлайн и адекватно справяне с бързо развиващия се проблем. Целта на тази законодателна рамка е да се използват доброволните усилия, които бяха засилени с Препоръка (ЕС) 2018/334 на Комисията[7], и да се отговори на призивите, отправени от Европейския парламент, за засилване на мерките за справяне с незаконното и вредното съдържание, както и на тези на Европейския съвет за подобряване на автоматизираното откриване и премахване на съдържание, което подбужда към терористични актове.

(5) Прилагането на настоящия регламент не следва да засяга прилагането на член 14 от Директива 2000/31/ЕО[8]. По-конкретно, всички мерки, предприети от доставчика на хостинг услуги в съответствие с настоящия регламент, включително всички проактивни мерки, не следва сами по себе си да водят до това доставчикът на услуги да загуби ползата от освобождаването от отговорност, предвидено в посочената разпоредба. Настоящият регламент не засяга правомощията на националните органи и съдилищата да определят отговорността на доставчиците на хостинг услуги в конкретни случаи, когато не са изпълнени условията по член 14 от Директива 2000/31/ЕО относно освобождаването от отговорност.

(6) В настоящия регламент са посочени правила за предотвратяване на злоупотребата с хостинг услуги с цел разпространение на терористично съдържание онлайн, чиято цел е да се гарантира безпрепятственото функциониране на вътрешния пазар при пълно зачитане на основните права, защитени в правния ред на Съюза, и по-специално тези, гарантирани в Хартата на основните права на Европейския съюз.

(7) Настоящият регламент допринася за защитата на обществената сигурност, като същевременно установява подходящи и стабилни гаранции за защитата на основните права. Това включва правото на зачитане на личния живот и защитата на личните данни, правото на ефективна съдебна защита, правото на свобода на изразяване, включително свободата на получаване и предаване на информация, свободата на стопанска инициатива и принципа на недискриминация. Компетентните органи и доставчиците на хостинг услуги следва да приемат

[7] Препоръка (ЕС) 2018/334 на Комисията от 1 март 2018 г. относно мерки за ефективна борба с незаконното съдържание онлайн (ОВ L 63, 6.3.2018 г., стр. 50).

[8] 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).

само мерки, които са необходими, подходящи и пропорционални в едно демократично общество, като вземат предвид особеното значение на свободата на изразяване на мнение и свободата на информация, която е един от фундаментите на плуралистичното и демократично общество, както и една от ценностите, на които се основава Съюзът. Мерките, представляващи намеса в свободата на изразяване на мнение и свободата на информация, следва да бъдат строго целеви, в смисъл че трябва да служат за предотвратяване на разпространението на терористично съдържание, без това да засяга правото на законно получаване и разпространяване на информация, като се взема предвид централната роля на доставчиците на хостинг услуги за способстването на обществения дебат и разпространението и получаването на факти, становища и идеи в съответствие със закона.

(8) Правото на ефективни правни средства за защита е залегнало в член 19 от ДЕС и в член 47 от Хартата на основните права на Европейския съюз. Всяко физическо или юридическо лице има право на ефективна съдебна защита пред компетентния национален съд срещу всяка мярка, предприета съгласно настоящия регламент, която може да засегне неблагоприятно правата на това лице. Правото включва, по-специално възможността доставчиците на хостинг услуги и доставчиците на съдържание да оспорват по ефективен начин заповедите за премахване на съдържание пред съда на държавата членка, чиито органи са издали такава заповед.

(9) С цел да се осигури яснота относно действията, които следва да предприемат както доставчиците на хостинг услуги, така и компетентните органи за предотвратяването на разпространението на терористично съдържание онлайн, в настоящия регламент следва да се установи определение за терористично съдържание за целите на предотвратяването въз основа на определението за терористични престъпления съгласно Директива (ЕС) 2017/541 на Европейския парламент и на Съвета[9]. Като се има предвид необходимостта да се обърне внимание на най-вредната терористична пропаганда онлайн, определението следва да обхваща материали и информация, които подбуждат, насърчават или пропагандират извършването на терористични престъпления или на съучастието в тях, предоставянето на указания за извършването на такива престъпления или подстрекаването към участие в дейности на терористична група. Тази информация включва по-конкретно текст, изображения, звукозаписи и видеозаписи. Когато преценяват дали съдържанието представлява терористично съдържание по смисъла на настоящия регламент, компетентните органи, както и доставчиците на хостинг услуги следва да вземат предвид фактори като естеството и формулировката на изявленията, контекста, в който са направени изявленията, и техния потенциал да доведат до вредни последици, засягащи по този начин сигурността и безопасността на хората. Фактът, че материалът е бил произведен от терористична организация или от лице, включени в списъка на ЕС, или че този материал им се приписва или е разпространяван от тяхно име, представлява важен фактор при преценката. Съдържание, което се разпространява за образователни, журналистически или научноизследователски цели, следва да бъде адекватно защитено. Освен това изразяването на радикални,

[9] 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).

полемични или противоречиви гледни точки в обществения дебат относно чувствителни политически въпроси не следва да се счита за терористично съдържание.

(10) С цел да се обхванат услугите за онлайн хостинг, с които се разпространява терористично съдържание, настоящият регламент следва да се прилага за услуги на информационното общество, които съхраняват информация, предоставена от получателя на услугата по негово искане, и при предоставянето на съхраняваната информация на разположение на трети страни, независимо дали тази дейност е чисто техническа, автоматизирана и пасивна. Например, такива доставчици на услуги на информационното общество включват платформи на социалните мрежи, услуги за видео стрийминг, услуги за споделяне на образ и звук, за споделяне на файлове и други услуги за изчисления в облак, доколкото предоставят информацията на трети страни, както и уебсайтове, където ползвателите могат да правят коментари или да публикуват отзиви. Регламентът следва да се прилага и за доставчици на хостинг услуги, установени извън Съюза, които предлагат услуги в рамките му, тъй като значителна част от доставчиците на хостинг услуги, изложени на терористично съдържание, са установени в трети държави. Така следва да се гарантира, че всички дружества, извършващи дейност на цифровия единен пазар, отговарят на същите изисквания, независимо в коя държава са установени. За да се установи дали даден доставчик на услуги предлага услуги в Съюза, е необходимо да се прецени дали доставчикът на услуги дава възможност на юридически или физически лица в една или няколко държави членки да използват услугите му. Самата достъпност на уебсайта на доставчика на услуги или на електронен адрес или на други координати за връзка в една или повече държави членки не следва обаче да е достатъчно условие за прилагането на настоящия регламент.

(11) За определянето на приложното поле на настоящия регламент значение следва да има наличието на съществена връзка със Съюза. Следва да се счита, че такава съществена връзка със Съюза съществува, когато доставчикът на услуги има място на установяване в Съюза или, при липса на такова, въз основа на наличието на значителен брой потребители в една или повече държави членки или на насочването на дейностите към една или повече държави членки. Насочването на дейностите към една или повече държави членки може да бъде определено въз основа на всички релевантни обстоятелства, включително фактори като използването на език или валута, които обикновено се използват в тази държава членка, или възможността за поръчване на стоки или услуги. Насочването на дейностите към дадена държава членка може също така да бъде изведено от наличието на приложение в съответния национален магазин за приложения, от предоставянето на местна реклама или реклама на езика, използван в тази държава членка, или начина на управляване на връзките с клиентите, като например чрез осигуряване на обслужване на клиентите на езика, който обикновено се използва в дадена държава членка. Също така следва да се приеме, че е налице съществена връзка, когато доставчикът на услуги насочва дейностите си към една или няколко държави членки, както е посочено в член 17, параграф 1, буква в) от Регламент (ЕО) № 1215/2012 на Европейския

парламент и на Съвета[10]. От друга страна, предоставянето на услугата само с оглед на спазването на забраната за дискриминация, определена в Регламент (ЕС) 2018/302 на Европейския парламент и на Съвета[11], не може да се разглежда единствено на това основание като насочване на дейностите към определена територия в рамките на Съюза.

(12) Доставчиците на хостинг услуги следва да изпълняват определени задължения за полагане на грижа с цел предотвратяване на разпространението на терористично съдържание чрез услугите им. Тези задължения за полагане на грижа не следва да представляват общо задължение за контрол. Задълженията за полагане на грижа следва да включват, че при прилагането на настоящия регламент, доставчиците на хостинг услуги действат по старателен, пропорционален и недискриминационен начин по отношение на съдържанието, което съхраняват, по-специално когато прилагат своите условия за ползване, за да се избегне премахването на съдържание, което не е терористично. Премахването или блокирането на достъпа трябва да се извършва при съблюдаване на свободата на изразяване на мнение и свободата на информация.

(13) Процедурата и задълженията, произтичащи от заповеди, с които на доставчиците на хостинг услуги се нарежда да премахнат терористично съдържание или да блокират достъпа до него, вследствие на преценка от страна на компетентните органи, следва да бъдат хармонизирани. Държавите членки следва да могат и занапред да избират своите компетентни органи, което им позволява да натоварят с тази задача административни, правоприлагащи или съдебни органи. Като се има предвид скоростта, с която терористичното съдържание се разпространява сред онлайн услугите, тази разпоредба налага задължения на доставчиците на хостинг услуги да гарантират, че терористичното съдържание, посочено в заповедта за премахване, е премахнато или че достъпът до него е бил блокиран в срок от един час от получаването на заповедта за премахване. Доставчиците на хостинг услуги са тези, които решават дали да премахнат това съдържание или да блокират достъпа до него за ползвателите в Съюза.

(14) Компетентният орган следва да предаде заповедта за премахване директно на адресата и звеното за контакт по всички електронни средства, които дават възможност за писмено документиране при условия, които позволяват на доставчика на услуги да установи автентичността, включително точността на датата и часа на изпращане и получаване на заповедта, например чрез защитена електронна поща и платформи или други защитени канали, включително предоставените от доставчика на услуги, в съответствие с правилата за защита на личните данни. Това изискване може да бъде изпълнено, по-специално чрез използването на квалифицирани услуги за електронна препоръчана поща, както

---

10 Регламент (ЕС) № 1215/2012 на Европейския парламент и на Съвета от 12 декември 2012 г. относно компетентността, признаването и изпълнението на съдебни решения по граждански и търговски дела (ОВ L 351, 20.12.2012 г., стр. 1).

11 Регламент (ЕС) 2018/302 на Европейския парламент и на Съвета от 28 февруари 2018 г. за преодоляване на необоснованото блокиране на географски принцип и на други форми на дискриминация въз основа на националността, местопребиваването или мястото на установяване на клиентите в рамките на вътрешния пазар и за изменение на регламенти (ЕО) № 2006/2004 и (ЕС) 2017/2394 и Директива 2009/22/ЕО (ОВ L 601, 2.3.2018 г., стр. 1).

е предвидено в Регламент (ЕС) № 910/2014 на Европейския парламент и на Съвета[12].

(15) Сигналите от компетентните органи или от Европол представляват ефективен и бърз начин за осведомяване на доставчиците на хостинг услуги за конкретно съдържание, на което са изложени услугите им. Този механизъм за предупреждаване на доставчиците на хостинг услуги относно информация, която може да се счита за терористично съдържание, с цел доставчикът доброволно да разгледа нейната съвместимост със собствените му условия за ползване, следва да остане на разположение в допълнение към заповедите за премахване. Важно е доставчиците на хостинг услуги да оценяват приоритетно такива сигнали и да предоставят бърза обратна информация за предприетите действия. Окончателното решение за това дали съдържанието да бъде премахнато или не, защото не е съвместимо с неговите условия за ползване, се взема от доставчика на хостинг услуги. При прилагането на настоящия регламент във връзка със сигналите, мандатът на Европол, определен в Регламент (ЕС) 2016/794[13], остава непроменен.

(16) Предвид мащаба и скоростта, необходими за ефективното откриване и премахване на терористично съдържание, наличието на пропорционални проактивни мерки, включително чрез използване на автоматизирани средства в някои случаи, е съществен елемент в борбата с терористичното съдържание онлайн. С цел намаляване на достъпността на терористичното съдържание, на което са изложени услугите им, доставчиците на хостинг услуги следва да преценят дали е целесъобразно да се предприемат проактивни мерки в зависимост от рисковете и степента на излагане на терористично съдържание, както и от въздействието върху правата на трети страни и обществения интерес от информация. Следователно доставчиците на хостинг услуги следва да определят каква подходяща, ефективна и пропорционална мярка следва да се въведе. Това задължение не следва да предполага наличието на общо задължение за контрол. В контекста на тази оценка липсата на заповеди за премахване и на сигнали, адресирани до доставчика на хостинг услуги, е признак за ниска степен на излагане на терористично съдържание.

(17) При въвеждането на проактивни мерки доставчиците на хостинг услуги следва да гарантират, че правото на ползвателите на свобода на изразяване на мнение и на свобода на информация, включително свобода на получаване и разпространяване на информация, се запазва. В допълнение към всички изисквания, предвидени в законодателството, включително законодателството за защита на личните данни, доставчиците на хостинг услуги следва да действат с дължима грижа и да прилагат гаранции, включително по-конкретно контрол и проверки от човек, когато това е целесъобразно, за да се избегне вземането на неволно и погрешно решение, водещо до премахване на съдържание, което не е терористично. Това е особено важно, когато доставчиците на хостинг услуги

---

12 Регламент (ЕС) № 910/2014 на Европейския парламент и на Съвета от 23 юли 2014 г. относно електронната идентификация и удостоверителните услуги при електронни трансакции на вътрешния пазар и за отмяна на Директива 1999/93/ЕО (ОВ L 257, 28.8.2014 г., стр. 73).

13 Регламент (ЕС) 2016/794 на Европейския парламент и на Съвета от 11 май 2016 г. относно Агенцията на Европейския съюз за сътрудничество в областта на правоприлагането (Европол) и за замяна и отмяна на решения 2009/371/ПВР, 2009/934/ПВР, 2009/935/ПВР, 2009/936/ПВР и 2009/968/ПВР на Съвета (ОВ L 135, 24.5.2016 г., стр. 53).

използват автоматизирани средства за откриване на терористично съдържание. Всяко решение за използване на автоматизирани средства, независимо дали е взето от самия доставчик на хостинг услуги или по искане на компетентния орган, следва да се оценява предвид надеждността на използваната технология и произтичащото от това въздействие върху основните права.

(18) За да се осигури, че доставчиците на хостинг услуги, изложени на терористично съдържание, предприемат подходящи мерки за предотвратяване на злоупотреба с техните услуги, компетентните органи следва да изискват от доставчиците на хостинг услуги, получили заповед за премахване, която е станала окончателна, да докладват за предприетите проактивни мерки. Те могат да представляват мерки за предотвратяване на повторно качване на терористично съдържание, което преди това е било премахнато или достъпът до което е бил блокиран вследствие на заповед за премахване или на получени от тях сигнали, проверени спрямо публично или частно притежавани инструменти, съдържащи известно терористично съдържание. Те могат също така да използват надеждни технически средства за идентифициране на ново терористично съдържание, като за целта използват наличните на пазара средства или тези, разработени от доставчика на хостинг услуги. Доставчикът на услуги следва да докладва за конкретните проактивни мерки, които прилага, за да се даде възможност на компетентния орган да прецени дали мерките са ефективни и пропорционални и дали, ако се използват автоматизирани средства, доставчикът на хостинг услуги притежава необходимия капацитет за извършване на контрол и проверка от човек. При оценяването на ефективността и пропорционалността на мерките компетентните органи следва да вземат предвид съответните параметри, включително броя на заповедите за премахване и на подадените до доставчика сигнали, икономическия му капацитет и въздействието на неговата услуга върху разпространението на терористично съдържание (например, като се вземе предвид броят на ползвателите в Съюза).

(19) В резултат на искането компетентният орган следва да започне диалог с доставчика на хостинг услуги относно необходимите проактивни мерки, които да бъдат въведени. Ако е необходимо, компетентният орган следва да наложи приемането на подходящи, ефективни и пропорционални проактивни мерки, когато счита, че предприетите мерки са недостатъчни за справяне с рисковете. Решението за налагане на такива конкретни проактивни мерки не следва по принцип да води до налагането на общо задължение за контрол, както е предвидено в член 15, параграф 1 от Директива 2000/31/ЕО. Като се имат предвид особено сериозните рискове, свързани с разпространението на терористично съдържание, решенията, приети от компетентните органи въз основа на настоящия регламент, могат да дерогират от подхода, установен в член 15, параграф 1 от Директива 2000/31/ЕО, по отношение на някои конкретни целеви мерки, чието приемане е необходимо поради причини, свързани с обществената сигурност. Преди приемането на такива решения компетентният орган следва да постигне справедлив баланс между целите от обществен интерес и свързаните с тях основни права, по-специално свободата на изразяване на мнение и свободата на информация и свободата на стопанска инициатива, както и да предостави подходяща обосновка.

(20) Задължението на доставчиците на хостинг услуги за запазване на премахнатото съдържание и на свързаните с него данни следва да бъде определено за конкретни цели и ограничено във времето до необходимото за тези цели.

Необходимо е изискването за запазване да се разшири до свързаните данни, доколкото тези данни иначе биха били загубени в резултат на премахването на въпросното съдържание. Свързаните данни могат да включват данни като „данни на абоната“, включително по-конкретно данни за самоличността на доставчика на съдържание, както и „данни за достъпа“, включително, например, данни за датата и часа на ползване от страна на доставчика на съдържание, или влизането и излизането от услугата, заедно с IP адреса, предоставен от доставчика на услуги за достъп до интернет на доставчика на съдържание.

(21) Задължението за запазване на съдържанието за целите на процедури за обжалване по административен или съдебен ред е необходимо и обосновано с цел да се гарантират ефективни мерки за правна защита за доставчика на съдържание, чието съдържание е било премахнато или достъпът до което е бил блокиран, както и за да се осигури възстановяването на това съдържание във вида му преди премахването в зависимост от резултата от процедурата за обжалване. Задължението за запазване на съдържание за целите на разследването и повдигането и поддържането на обвинение е обосновано и необходимо с оглед на важността, която този материал би могъл да има за възпрепятстването или предотвратяването на терористичната дейност. Когато предприятия премахват или блокират достъпа до съдържание, по-специално чрез свои собствени проактивни мерки, но не информират съответния орган за това, тъй като преценяват, че то не попада в приложното поле на член 13, параграф 4 от настоящия регламент, правоприлагащите органи може да не знаят за съществуването на съдържанието. Поради това запазването на съдържанието за целите на предотвратяването, откриването, разследването и наказателното преследване на терористични престъпления също е оправдано. За тези цели изискваното съхранение на данни е ограничено до данни, които е вероятно да имат връзка с терористични престъпления, и следователно може да допринесат за наказателното преследване на терористични престъпления или за предотвратяването на сериозни рискове за обществената сигурност.

(22) За да се гарантира пропорционалността, периодът на съхранение следва да бъде ограничен до шест месеца, за да се даде достатъчно време на доставчиците на съдържание да започнат процеса на обжалване и да се даде възможност на правоприлагащите органи да получат достъп до съответните данни от значение за разследването и наказателното преследване на терористични престъпления. Въпреки това този срок може да бъде удължен за периода, който е необходим, в случай че процедурата по обжалване е започнала, но не е приключила в рамките на шестмесечния срок по искане на органа, занимаващ се с обжалването. Тази продължителност следва да бъде достатъчна, за да се даде възможност на правоприлагащите органи да запазят необходимите доказателства във връзка с разследванията, като същевременно се гарантира балансът със съответните основни права.

(23) Настоящият регламент не засяга процесуалните гаранции и процедурните мерки за разследване, свързани с достъпа до съдържание и свързаните с него данни, съхранявани за целите на разследването и наказателното преследване на терористични престъпления, уредени съгласно националното законодателство на държавите членки и съгласно законодателството на Съюза.

(24) Прозрачността на политиките на доставчиците на хостинг услуги във връзка с терористичното съдържание е от съществено значение за подобряване на тяхната отчетност спрямо техните ползватели и за укрепване на доверието на

гражданите в цифровия единен пазар. Доставчиците на хостинг услуги следва да публикуват годишни доклади за прозрачност, съдържащи полезна информация за предприетите действия във връзка с откриването, идентифицирането и премахването на терористично съдържание.

(25) Процедурите за подаване на жалби представляват необходима предпазна мярка срещу погрешното премахване на съдържание, защитено съгласно свободата на изразяване на мнение и свободата на информация. Поради това доставчиците на хостинг услуги следва да създадат удобни за ползвателите механизми за подаване на жалби и да гарантират, че жалбите се обработват бързо и при пълна прозрачност спрямо доставчика на съдържание. Изискването доставчикът на хостинг услуги да възстанови съдържанието, когато то е било премахнато поради грешка, не засяга възможността доставчиците на хостинг услуги да прилагат своите условия за ползване на други основания.

(26) Съгласно член 19 от ДЕС и член 47 от Хартата на основните права на Европейския съюз ефективната правна защита изисква лицата да са в състояние да установят какви са причините, поради които съдържанието, качено от тях, е било премахнато или достъпът до него е бил блокиран. За тази цел доставчикът на хостинг услуги следва да предостави на разположение на доставчика на съдържание смислена информация, позволяваща на доставчика на съдържание да оспори решението. Това обаче не изисква непременно уведомяване на доставчика на съдържанието. В зависимост от обстоятелствата доставчиците на хостинг услуги могат да заменят съдържанието, което се счита за терористично съдържание, със съобщение, че то е било премахнато или че достъпът до него е бил блокиран в съответствие с настоящия регламент. Допълнителна информация за причините, както и за възможностите доставчикът на съдържание да оспори решението, следва да бъде предоставена при поискване. Когато компетентните органи решат, че по причини, свързани с обществената сигурност, включително в рамките на разследване, се счита, че не е целесъобразно или ще има обратен ефект доставчикът на съдържание да бъде директно уведомен за премахването на съдържание или за блокирането на достъпа до него, те следва да уведомят за това доставчика на хостинг услуги.

(27) За да се избегне дублирането на работа и възможната намеса в разследвания, компетентните органи следва взаимно да се уведомяват и координират и да си сътрудничат помежду си и, когато е целесъобразно, с Европол, при издаването на заповеди за премахване или при изпращането на сигнали до доставчици на хостинг услуги. При прилагането на разпоредбите на настоящия регламент Европол може да окаже подкрепа в съответствие със сегашния си мандат и съществуващата правна уредба.

(28) За да се осигури ефективно и достатъчно съгласувано прилагане на проактивни мерки, компетентните органи в държавите членки следва да си сътрудничат по отношение на дискусиите, които водят с доставчиците на хостинг услуги във връзка с установяването, прилагането и оценката на конкретни проактивни мерки. Подобно сътрудничество е необходимо и във връзка с приемането на правила относно санкциите, както и във връзка с изпълнението и налагането на санкции.

(29) От съществено значение е компетентният орган в държавата членка, който отговаря за налагането на санкции, да бъде напълно информиран за издаването на заповеди за премахване и за подаването на сигнали, както и за последващ

обмен между доставчика на услуги и съответния компетентен орган. За тази цел държавите членки предоставят подходящи канали или механизми за комуникация, позволяващи своевременното споделяне на съответната информация.

(30) За да се улесни бързият обмен на информация между компетентните органи, както и с доставчиците на хостинг услуги, а също и за да се избегне дублирането на усилия, държавите членки могат да използват разработените от Европол инструменти, като например действащото приложение за управление на сигнализирането в интернет (Internet Referral Management application (IRMa) или инструменти, които са негови приемници.

(31) Предвид конкретните сериозни последици от определено терористично съдържание доставчиците на хостинг услуги следва незабавно да уведомяват съответните органи в засегнатата държава членка или компетентните органи на мястото, където се намира тяхното основно място на стопанска дейност или законният им представител, за съществуването на доказателства за терористични престъпления, за които са узнали. За да се гарантира пропорционалността, това задължение е ограничено до терористичните престъпления, определени в член 3, параграф 1 от Директива (ЕС) 2017/541. Задължението за уведомяване не предполага задължение за доставчиците на хостинг услуги активно да търсят такива доказателства. Засегнатата държава членка е държавата членка, която има юрисдикция при разследването и наказателното преследване на терористичните престъпления в съответствие с Директива (ЕС) 2017/541, въз основа на гражданството на извършителя на престъплението или на потенциалната жертва на престъплението или на мястото на извършване на терористичния акт. В случай на съмнение доставчиците на хостинг услуги могат да предават информацията на Европол, който следва да действа в съответствие със своя мандат, включително да препраща информацията на съответните национални органи.

(32) Компетентните органи в държавите членки следва да могат да използват тази информация, за да предприемат мерки за разследване, които са предвидени съгласно правото на държава членка или на Съюза, включително издаването на европейска заповед за предоставяне съгласно Регламента относно европейските заповеди за предоставяне и за запазване на електронни доказателства по наказателноправни въпроси[14].

(33) Както доставчиците на хостинг услуги, така и държавите членки следва да създадат звена за контакт, които да улесняват бързото обработване на заповедите за премахване и на сигналите. За разлика от законния представител звеното за контакт служи за оперативни цели. Звеното за контакт на доставчика на хостинг услуги следва да разполага със специализирани средства, позволяващи подаването на заповеди за премахване и на сигнали по електронен път, както и с технически средства и персонал, позволяващи бързото им обработване. Не е необходимо звеното за контакт на доставчика на хостинг услуги да се намира в Съюза, като доставчикът на хостинг услуги е свободен да определи съществуващо звено за контакт, при условие че то може да изпълнява функциите, предвидени в настоящия регламент. С цел да се гарантира, че дадено терористично съдържание е премахнато или че достъпът до него е блокиран в

[14] COM(2018)225 final.

срок от един час след получаване на заповед за премахване, доставчиците на хостинг услуги следва да гарантират, че звеното за контакт е на разположение 24 часа в денонощието седем дни в седмицата. Информацията относно звеното за контакт следва да включва информация относно езика, на който може да се общува с него. С цел да се улесни комуникацията между доставчиците на хостинг услуги и компетентните органи, доставчиците на хостинг услуги се насърчават да позволяват комуникация на един от официалните езици на Съюза, на който са налични техните условия за ползване.

(34) При липсата на общо изискване доставчиците на услуги да гарантират физическо присъствие на територията на Съюза е необходимо да се осигури яснота относно това коя държава членка има юрисдикция по отношение на доставчика на хостинг услуги, предлагащ услуги в рамките на Съюза. Като общо правило доставчикът на хостинг услуги попада под юрисдикцията на държавата членка, в която се намира неговото основно място на стопанска дейност или в която е установен неговият законен представител. Независимо от това, когато друга държава членка издаде заповед за премахване, нейните органи следва да могат да налагат изпълнението на своите заповеди, като предприемат принудителни мерки с ненаказателен характер, като например плащането на глоби. По отношение на доставчик на хостинг услуги,който не е установен в Съюза и който не е определил законен представител, всяка държава членка следва да може да налага санкции, при условие че се спазва принципът *ne bis in idem*.

(35) Доставчиците на хостинг услуги, които не са установени в Съюза, следва да определят писмено законен представител с цел да гарантират спазването и изпълнението на задълженията съгласно настоящия регламент.

(36) Законният представител следва да бъде законно упълномощен да действа от името на доставчика на хостинг услуги.

(37) За целите на настоящия регламент държавите членки следва да определят компетентни органи. Изискването за определяне на компетентни органи не означава непременно създаването на нови органи, а може да представлява възлагане на изпълнението на функциите, определени в настоящия регламент, на съществуващи органи. Настоящият регламент налага определянето на органи, компетентни да издават заповеди за премахване и сигнали, както и да следят за прилагането на проактивни мерки и за налагането на санкции. Държавите членки решават колко органа да определят за изпълнението на тези задачи.

(38) Необходими са санкции, за да се гарантира ефективното изпълнение от страна на доставчиците на хостинг услуги на задълженията съгласно настоящия регламент. Държавите членки следва да приемат правила относно санкциите, включително, когато е целесъобразно, насоки за налагане на глоби. Особено тежки санкции следва да се налагат, в случай че доставчикът на хостинг услуги систематично не премахва терористично съдържание или не блокира достъпа до него в срок от един час от получаването на заповедта за премахване. Неспазването на изискванията в отделни случаи може да бъде санкционирано, като същевременно се спазват принципите на *ne bis in idem* и на пропорционалност и като се гарантира, че при тези санкции се взема предвид систематичното неспазване. За да се гарантира правната сигурност, в регламента следва да се определи до каква степен съответните задължения могат да бъдат предмет на санкции. Санкциите за неспазване на разпоредбите на член 6 следва

да се приемат единствено във връзка със задължения, произтичащи от искане за докладване съгласно член 6, параграф 2 или решение за налагане на допълнителни проактивни мерки съгласно член 6, параграф 4. При определяне на това дали следва да бъдат наложени финансови санкции, следва да се вземат предвид финансовите ресурси на доставчика. Държавите членки следва да гарантират, че санкциите не насърчават премахването на съдържание, което не е терористично съдържание.

(39) Използването на стандартизирани образци улеснява сътрудничеството и обмена на информация между компетентните органи и доставчиците на услуги, като им позволява да общуват по-бързо и по-ефективно. Особено важно е да се гарантират бързи действия след получаването на заповед за премахване. Благодарение на образците се намаляват разходите за превод и се допринася за установяването на стандарт за високо качество. Формулярите за отговор следва да направят възможен стандартизирния обмен на информация,а това ще бъде от голямо значение, когато доставчиците на услуги не могат да спазяят изискванията. Каналите за подаване с удостоверена автентичност могат да гарантират автентичността на заповедта за премахване, включително точността на датата и часа на изпращане и получаване на заповедта.

(40) С цел да се даде възможност за бързо изменение, когато е необходимо, на съдържанието на образците, които да бъдат използвани за целите на настоящия регламент, на Комисията следва да бъде делегирано правомощието да приема актове в съответствие с член 290 от Договора за функционирането на Европейския съюз за изменение на приложения I, II и III към настоящия регламент. За да може да взема предвид развитието на технологиите и свързаната с това правна уредба, на Комисията следва да се предостави правомощието да приема делегирани актове с цел допълване на настоящия регламент с техническите изисквания за електронните средства, които да се използват от компетентните органи за връчването на заповедите за премахване. От особена важност е по време на своята подготвителна работа Комисията да проведе подходящи консултации, включително на експертно равнище, и тези консултации да бъдат проведени в съответствие с принципите, заложени в Междуинституционалното споразумение за по-добро законотворчество от 13 април 2016 г.[15] По-специално, с цел осигуряване на равно участие при подготовката на делегираните актове, Европейският парламент и Съветът получават всички документи едновременно с експертите от държавите членки, като техните експерти получават систематично достъп до заседанията на експертните групи на Комисията, занимаващи се с подготовката на делегираните актове.

(41) Държавите членки следва да събират информация относно прилагането на законодателството. Следва да се създаде подробна програма за мониторинг на крайните продукти, резултатите и въздействието на настоящия регламент, като целта е информацията от нея да се използва за оценка на законодателството.

(42) Въз основа на констатациите и заключенията в доклада за изпълнението и на резултата от мониторинга Комисията следва да извърши оценка на настоящия регламент не по-рано от три години след влизането му в сила. Оценката следва да се основава на петте критерия за ефикасност, ефективност, уместност,

[15] ОВ L 123, 12.5.2016 г., стр. 1.

съгласуваност и добавена стойност от ЕС. С нея ще се оцени функционирането на различните оперативни и технически мерки, предвидени в Регламента, включително ефективността на мерките за подобряване на откриването, идентифицирането и премахването на терористично съдържание, ефективността на предпазните механизми, както и въздействието върху потенциално засегнатите права и интереси на трети страни, включително преглед на изискването за информиране на доставчиците на съдържание.

(43) Тъй като целта на настоящия регламент, а именно да се гарантира безпрепятственото функциониране на цифровия единен пазар чрез предотвратяване на разпространението на терористично съдържание онлайн, не може да бъде постигната в достатъчна степен от държавите членки и следователно, поради обхвата и последиците от предвиденото действие, може да бъде по-добре постигната на равнището на Съюза, Съюзът може да приеме мерки в съответствие с принципа на субсидиарност, уреден в член 5 от Договора за Европейския съюз. В съответствие с принципа на пропорционалност, уреден в същия член, настоящият регламент не надхвърля необходимото за постигането на тази цел,

ПРИЕХА НАСТОЯЩИЯ РЕГЛАМЕНТ:

РАЗДЕЛ I
ОБЩИ РАЗПОРЕДБИ

Член 1
Предмет и приложно поле

1. С настоящия регламент се установяват единни правила за предотвратяване на злоупотребата с хостинг услуги за разпространение на терористично съдържание онлайн. С него се установяват по-специално:

   а) правила относно задълженията на доставчиците на хостинг услуги да полагат грижи за предотвратяване на разпространението на терористично съдържание чрез техните услуги и да гарантират, когато е необходимо, бързото му премахване;

   б) набор от мерки, които да бъдат въведени от държавите членки с цел идентифициране на терористично съдържание, гарантиране на бързото му премахване от доставчиците на хостинг услуги и улесняване на сътрудничеството с компетентните органи в други държави членки, доставчици на хостинг услуги и, когато е целесъобразно, съответните органи на Съюза.

2. Настоящият регламент се прилага за доставчиците на хостинг услуги, които предлагат услуги в Съюза, независимо от тяхното основно място на стопанска дейност.

Член 2
Определения

За целите на настоящия регламент се прилагат следните определения:

1) „доставчик на хостинг услуги“ означава доставчик на услуги на информационното общество, които се състоят в съхраняването по искане на

доставчика на съдържание на информация, предоставяна от самия него, и в предоставяне на съхраняваната информация на разположение на трети страни;

2) „доставчик на съдържание“ означава ползвател, предоставил информация, която се съхранява или е била съхранявана по негово искане от доставчик на хостинг услуги;

3) „предлагане на услуги в Съюза“ означава предоставяне на възможността юридически или физически лица в една или няколко държави членки да използват услугите на доставчика на хостинг услуги, който има съществена връзка с тази държава членка или тези държави членки, изразяваща се във:

   а) установяване на доставчика на хостинг услуги в Съюза;

   б) значителен брой ползватели в една или няколко държави членки;

   в) насочване на дейностите към една или няколко държави членки.

4) „терористични престъпления“ означава престъпления по смисъла на член 3, параграф 1 от Директива (ЕС) 2017/541;

5) „терористично съдържание“ означава информация от един или няколко от следните видове:

   а) информация, с която се подбужда към или се пропагандира, включително чрез възхвала, извършването на терористични престъпления, като по този начин се създава опасност от извършването на такива деяния;

   б) информация, с която се насърчава съучастието в терористични престъпления;

   в) информация, с която се популяризират дейностите на терористична група, по-специално като се насърчава участието или подкрепата за терористична група по смисъла на член 2, параграф 3 от Директива (ЕС) 2017/541;

   г) информация, с която се дават указания относно методи или техники за извършване на терористични престъпления.

6) „разпространение на терористично съдържание“ означава предоставяне на терористично съдържание на разположение на трети страни чрез услугите на доставчици на хостинг услуги;

7) „условия за ползване“ означава всички условия и клаузи, независимо от тяхното наименование или форма, с които се уреждат договорните отношения между доставчика на хостинг услуги и ползвателите на тези услуги;

8) „сигнал“ означава известие от компетентен орган или, когато е приложимо, от компетентен орган на Съюза до доставчик на хостинг услуги относно информация, която може да се счита за терористично съдържание, с цел доставчикът доброволно да разгледа нейната съвместимост със собствените му условия за ползване, които имат за цел предотвратяване на разпространението на терористично съдържание;

9) „основно място на стопанска дейност“ означава главното управление или седалището, в което се упражняват основните финансови функции и оперативният контрол.

РАЗДЕЛ II
Мерки за предотвратяване на разпространението на терористично съдържание онлайн

Член 3
Задължения за полагане на грижа

1. Доставчиците на хостинг услуги предприемат целесъобразни, разумни и пропорционални действия в съответствие с настоящия регламент срещу разпространението на терористично съдържание и за защита на ползвателите от терористично съдържание. При това те действат по старателен, пропорционален и недискриминационен начин, като зачитат надлежно основните права на ползвателите и вземат предвид фундаменталното значение на свободата на изразяване на мнение и свободата на информация в едно отворено и демократично общество.

2. Доставчиците на хостинг услуги включват в своите условия за ползване разпоредби за предотвратяване на разпространението на терористично съдържание и ги прилагат.

Член 4
Заповеди за премахване

1. Компетентният орган разполага с правомощието да постанови решение, с което да изиска от доставчика на хостинг услуги да премахне терористично съдържание или да блокира достъпа до него.

2. Доставчиците на хостинг услуги премахват терористично съдържание или блокират достъпа до него в срок от един час след получаването на заповедта за премахване.

3. Заповедите за премахване съдържат следните елементи в съответствие с образеца, установен в приложение I:

   а) данни за компетентния орган, издаващ заповедта за премахване, и удостоверение на автентичността на заповедта за премахване от компетентния орган;

   б) описание на причините, поради които съдържанието се счита за терористично съдържание, най-малкото чрез позоваване на категориите терористично съдържание, изброени в член 2, параграф 5;

   в) унифициран локатор на ресурси (URL) и, когато е необходимо, допълнителна информация, която позволява да се идентифицира въпросното съдържание;

   г) позоваване на настоящия регламент като правното основание на заповедта за премахване;

   д) дата и времеви печат за момента на издаване;

   е) информация относно средствата за правна защита, които са на разположение на доставчика на хостинг услуги и доставчика на съдържание;

ж) когато е приложимо, решението да не се оповестява информацията относно премахването на терористично съдържание или блокирането на достъпа до него, както е посочено в член 11.

4. По искане на доставчика на хостинг услуги или на доставчика на съдържание компетентният орган представя подробно описание на причините, без да се засяга задължението на доставчика на хостинг услуги да изпълни заповедта за премахване в рамките на срока, посочен в параграф 2.

5. Компетентните органи отправят заповедите за премахване към основното място на стопанска дейност на доставчика на хостинг услуги или към законния представител, определен от доставчика на хостинг услуги съгласно член 16, и ги препращат на звеното за контакт, посочено в член 14, параграф 1. Тези заповеди се изпращат с електронни средства, които дават възможност за писмено документиране при условия, които позволяват установяване на автентичността на изпращача, включително точността на датата и часа на изпращане и получаване на заповедта.

6. Доставчиците на хостинг услуги потвърждават получаването и без ненужно забавяне информират компетентния орган за премахването на терористичното съдържание или за блокирането на достъпа до него, като посочват по-специално часа и датата на предприетото действие, използвайки образеца от приложение II.

7. Ако доставчикът на хостинг услуги не може да изпълни заповедта за премахване поради непреодолима сила или фактическа невъзможност, която не се дължи на доставчика на хостинг услуги, той информира без ненужно забавяне компетентния орган за това, като обяснява причините, използвайки образеца от приложение III. Крайният срок, посочен в параграф 2, се прилага веднага щом посочените причини престанат да съществуват.

8. Ако доставчикът на хостинг услуги не може да изпълни заповедта за премахване, тъй като в нея се съдържат явни грешки или не се съдържа достатъчно информация за изпълнение на заповедта, доставчикът на хостинг услуги уведомява без ненужно забавяне компетентния орган за това, като изисква пояснения, използвайки образеца от приложение III. Крайният срок, посочен в параграф 2, се прилага веднага щом посочените пояснения бъдат предоставени.

9. Компетентният орган, издал заповедта за премахване, информира компетентния орган, който следи за прилагането на проактивните мерки, посочени в член 17, параграф 1, буква в), когато заповедта за премахване стане окончателна. Дадена заповед за премахване става окончателна, когато не е била обжалвана в рамките на срока, предвиден за това в приложимото национално законодателство, или когато е била потвърдена след обжалване.

Член 5
Сигнали

1. Компетентният орган или съответният орган на Съюза може да изпрати сигнал до доставчик на хостинг услуги.

2. Доставчиците на хостинг услуги въвеждат оперативни и технически мерки, с които се улеснява експедитивната оценка на съдържанието, изпратено за

доброволно разглеждане от тяхна страна от компетентните органи и, когато е приложимо, от съответните органи на Съюза.

3. Сигналите се отправят към основното място на стопанска дейност на доставчика на хостинг услуги или на законния представител, определен от доставчика на хостинг услуги съгласно член 16, и се препращат на звеното за контакт, посочено в член 14, параграф 1. Тези сигнали се изпращат по електронен път.

4. Сигналът съдържа достатъчно подробна информация, включително причините, поради които съдържанието се счита за терористично съдържание, URL и, когато е необходимо, допълнителна информация, която позволява да се идентифицира въпросното терористично съдържание.

5. Доставчикът на хостинг услуги оценява приоритетно съдържанието, посочено в сигнала, спрямо своите условия за ползване и решава дали да премахне това съдържание или да блокира достъпа до него.

6. Доставчикът на хостинг услуги уведомява своевременно компетентния орган или съответния орган на Съюза за резултата от оценката и точния момент на всяко действие, предприето вследствие на сигнала.

7. Когато доставчикът на хостинг услуги счита, че сигналът не съдържа достатъчно информация, за да се направи оценка на въпросното съдържание, той незабавно уведомява компетентните органи или съответния орган на Съюза за това, като посочва какви допълнителни сведения или пояснения са необходими.

Член 6
Проактивни мерки

1. Когато е целесъобразно, доставчиците на хостинг услуги предприемат проактивни мерки, за да предпазят своите услуги от разпространението на терористично съдържание. Мерките са ефективни и пропорционални, като отчитат риска и равнището на излагане на терористично съдържание, основните права на ползвателите и фундаменталното значение на свободата на изразяване на мнение и свободата на информация в едно отворено и демократично общество.

2. Когато е бил информиран в съответствие с член 4, параграф 9, компетентният орган, посочен в член 17, параграф 1, буква в), изисква от доставчика на хостинг услуги да представи доклад в срок от три месеца след получаване на искането и след това най-малко веднъж годишно във връзка с конкретните проактивни мерки, които е предприел, включително чрез използването на автоматизирани инструменти, с цел:

   а) предотвратяването на повторно качване на съдържание, което преди това е било премахнато или достъпът до което е бил блокиран, тъй като се счита за терористично съдържание;

   б) откриването, идентифицирането и експедитивното премахване на терористично съдържание или блокиране на достъпа до него.

   Това искане се изпраща до основното място на стопанска дейност на доставчика на хостинг услуги или на законния представител, определен от доставчика на хостинг услуги.

Докладите включват цялата относима информация, която позволява на компетентния орган, посочен в член 17, параграф 1, буква в), да прецени дали проактивните мерки са ефективни и пропорционални, включително да оцени функционирането на всички използвани автоматизирани инструменти, както и използваните механизми за контрол и проверка от човек.

3. Когато компетентният орган, посочен в член 17, параграф 1, буква в), счита, че предприетите проактивни мерки, за които е докладвано съгласно параграф 2, не са достатъчни за ограничаването и управлението на риска и равнището на излагане, той може да поиска от доставчика на хостинг услуги да предприеме конкретни допълнителни проактивни мерки. За тази цел доставчикът на хостинг услуги си сътрудничи с компетентния орган, посочен в член 17, параграф 1, буква в), за да се определят конкретните мерки, които доставчикът на хостинг услуги да въведе, като се установяват ключови цели и критерии, както и графици за тяхното изпълнение.

4. Ако не може да бъде постигнато споразумение в рамките на три месеца от искането по параграф 3, компетентният орган, посочен в член 17, параграф 1, буква в), може да издаде решение, с което да наложи конкретни допълнителни необходими и пропорционални проактивни мерки. В решението се вземат предвид по-специално икономическият капацитет на доставчика на хостинг услуги и ефектът от такива мерки върху основните права на ползвателите и фундаменталното значение на свободата на изразяване на мнение и свободата на информация. Това решение се изпраща до основното място на стопанска дейност на доставчика на хостинг услуги или на законния представител, определен от доставчика на хостинг услуги. Доставчикът на хостинг услуги редовно докладва за изпълнението на тези мерки, както е определено от компетентния орган, посочен в член 17, параграф 1, буква в).

5. Доставчикът на хостинг услуги може по всяко време да поиска от компетентния орган, посочен в член 17, параграф 1, буква в), да преразгледа и при необходимост да отмени дадено искане или решение по параграфи 2, 3 и 4 съответно. Компетентният орган издава мотивирано решение в рамките на разумен срок след получаване на искането от доставчика на хостинг услуги.

Член 7

Съхраняване на съдържание и свързани с него данни

1. Доставчиците на хостинг услуги съхраняват терористичното съдържание, което е премахнато или блокирано вследствие на заповед за премахване, сигнал или проактивни мерки в съответствие с членове 4, 5 и 6, и свързаните с него данни, които са премахнати в резултат на премахването на терористичното съдържание и които са необходими за:

   а) процедури за обжалване по административен или съдебен ред,

   б) предотвратяването, разкриването, разследването или наказателното преследване на терористични престъпления;

2. Терористичното съдържание и свързаните с него данни, посочени в параграф 1, се съхраняват за срок от шест месеца. При поискване от компетентния орган или съд терористичното съдържание се съхранява за по-дълъг период, когато и докато това е необходимо за текущи процедури за обжалване по административен или съдебен ред, посочени в параграф 1, буква а).

3. Доставчиците на хостинг услуги гарантират, че терористичното съдържание и свързаните с него данни, съхранявани съгласно параграфи 1 и 2, са предмет на подходящи технически и организационни предпазни мерки.

С тези технически и организационни предпазни мерки се гарантира, че съхраняваното терористично съдържание и свързаните с него данни са достъпни и се обработват само за целите, посочени в параграф 1, и се осигурява висока степен на сигурност на засегнатите лични данни. Доставчиците на хостинг услуги преразглеждат и актуализират тези предпазни мерки, когато е необходимо.

РАЗДЕЛ III
ПРЕДПАЗНИ МЕРКИ И ОТЧЕТНОСТ

Член 8

Задължения за прозрачност

1. Доставчиците на хостинг услуги установяват в своите условия за ползване политиката си за предотвратяване на разпространението на терористично съдържание, включително, когато е целесъобразно, с подходящо обяснение за функционирането на проактивните мерки, в това число използването на автоматизирани инструменти.

2. Доставчиците на хостинг услуги публикуват годишни доклади за прозрачност относно действията, предприети срещу разпространението на терористично съдържание.

3. Докладите за прозрачност съдържат най-малко следната информация:

   а) информация относно мерките на доставчика на хостинг услуги във връзка с откриването, идентифицирането и премахването на терористично съдържание;

   б) информация относно мерките на доставчика на хостинг услуги за предотвратяване на повторно качване на съдържание, което преди това е било премахнато или достъпът до което е бил блокиран, тъй като се счита за терористично съдържание;

   в) брой на материалите с терористично съдържание, които са били премахнати или достъпът до които е бил блокиран вследствие съответно на заповеди за премахване, сигнали или проактивни мерки;

   г) обзор и резултати от процедурите за подаване на жалби.

Член 9

Гаранции по отношение на използването и прилагането на проактивните мерки

1. Когато доставчиците на хостинг услуги използват автоматизирани средства съгласно настоящия регламент по отношение на съдържанието, което съхраняват, те предоставят ефективни и подходящи гаранции за точността и обосноваността на решенията, вземани във връзка с това съдържание, и по-специално на решенията за премахване на съдържание, което се счита за терористично, или за блокирането на достъпа до него.

2. Тези гаранции се изразяват по-конкретно в контрол и проверки от човек, 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 терористично.

Член 10

Механизми за подаване на жалби

1. Доставчиците на хостинг услуги установяват ефективни и достъпни механизми, позволяващи на доставчиците на съдържание, чието съдържание е било премахнато или до което е бил блокиран достъпът вследствие на сигнал съгласно член 5 или на проактивни мерки съгласно член 6, да подадат жалба срещу действието на доставчика на хостинг услуги с искане съдържанието да бъде възстановено.

2. Доставчиците на хостинг услуги разглеждат своевременно всяка получена жалба и възстановяват съдържанието без ненужно забавяне, когато премахването или блокирането на достъпа е било неоснователно. Те информират жалбоподателя за резултата от разглеждането на жалбата.

Член 11

Информация за доставчиците на съдържание

1. Когато доставчиците на хостинг услуги премахват терористично съдържание или блокират достъпа до него, те предоставят на доставчика на съдържание информация относно премахването или блокирането на достъпа до терористично съдържание.

2. При поискване от доставчика на съдържание доставчикът на хостинг услуги информира доставчика на съдържание за причините за премахването или блокирането на достъпа и за възможностите за оспорване на решението.

3. Задължението съгласно параграфи 1 и 2 не се прилага, когато компетентният орган реши, че тези дейности не бива да бъдат оповестявани поради причини, свързани с обществената сигурност, като например предотвратяването, разследването, разкриването и наказателното преследване на терористични престъпления, за толкова дълго време, колкото е необходимо, но не повече от [четири] седмици от това решение. В такъв случай доставчикът на хостинг услуги не оповестява никаква информация за премахването или блокирането на достъпа до терористично съдържание.

РАЗДЕЛ IV
Сътрудничество между компетентните органи, органите на Съюза и доставчиците на хостинг услуги

Член 12

Капацитет на компетентните органи

Държавите членки гарантират, че техните компетентни органи разполагат с необходимия капацитет и с достатъчни ресурси за постигане на целите и за изпълнение на техните задълженията по настоящия регламент.

Член 13

Сътрудничество между доставчиците на хостинг услуги, компетентните органи и когато е необходимо, съответните органи на Съюза

1. Компетентните органи в държавите членки взаимно се уведомяват и координират и си сътрудничат помежду си и, когато е целесъобразно, със съответните органи на Съюза, като например Европол, по отношение на заповедите за премахване и сигналите, за да се избегне дублирането на работа, да се подобри координацията и да се избегне намесата в разследвания в различните държави членки.

2. Компетентните органи в държавите членки информират, координират и си сътрудничат с компетентния орган, посочен в член 17, параграф 1, букви в) и г), по отношение на мерките, предприети съгласно член 6, и мерките за принудително изпълнение съгласно член 18. Държавите членки гарантират, че компетентният орган, посочен в член 17, параграф 1, букви в) и г), притежава цялата необходима информация. За тази цел държавите членки предоставят подходящи канали или механизми за комуникация, за да се гарантира, че съответната информация се обменя своевременно.

3. Държавите членки и доставчиците на хостинг услуги могат да решат да използват специални инструменти, включително, когато е целесъобразно, тези, създадени от съответните органи на Съюза, като например Европол, за да се улеснят по-специално:

   а) обработването и обратната информация, свързани със заповеди за премахване в съответствие с член 4;

   б) обработването и обратната информация, свързани със сигнали в съответствие с член 5;

   в) сътрудничество с цел определянето и прилагането на проактивни мерки в съответствие с член 6.

4. Когато доставчиците на хостинг услуги узнаят за доказателства за терористични престъпления, те незабавно уведомяват органите, компетентни за разследването и наказателното преследване на престъпления в съответната държава членка или звеното за контакт в държавата членка съгласно член 14, параграф 2, в която се намира тяхното основно място на стопанска дейност или законният им представител. В случай на съмнение доставчиците на хостинг услуги могат да предават тази информация на Европол за съответни последващи действия.

Член 14

Звена за контакт

1. Доставчиците на хостинг услуги създават звено за контакт, което получава заповедите за премахване и сигналите по електронен път и осигурява бързото им обработване съгласно членове 4 и 5. Те гарантират, че тази информация е обществено достояние.

2. В информацията, посочена в параграф 1, се посочва официалният език или официалните езици на Съюза съгласно Регламент (ЕС) № 1/58, на който може да се общува със звеното за контакт и на който се обменя допълнителна информация във връзка със заповедите за премахване и сигналите съгласно

членове 4 и 5. Това включва поне един от официалните езици на държавата членка, в която се намира основното място на стопанска дейност на доставчика на хостинг услуги или е установен или пребивава неговият законен представител съгласно член 16.

3. Държавите членки създават звено за контакт, което обработва исканията за разяснения и обратна информация във връзка с издадените от тях заповеди за премахване и подадените от тях сигнали. Информацията относно звеното за контакт се прави обществено достояние.

РАЗДЕЛ V
ИЗПЪЛНЕНИЕ И ПРИЛАГАНЕ

Член 15
Юрисдикция

1. За целите на членове 6, 18 и 21 юрисдикция има държавата членка, в която се намира основно място на стопанска дейност на доставчика на хостинг услуги. За доставчик на хостинг услуги, който няма основно място на стопанска дейност в никоя държава членка, се счита, че е под юрисдикцията на държавата членка, в която пребивава или е установен неговият законен представител, посочен в член 16.

2. Когато доставчик на хостинг услуги не е определил свой законен представител, всички държави членки имат юрисдикция.

3. Когато орган на друга държава членка е издал заповед за премахване в съответствие с член 4, параграф 1, тази държава членка има юрисдикция да предприеме принудителни мерки съгласно своето национално право с цел изпълнението на заповедта за премахване.

Член 16
Законен представител

1. Доставчик на хостинг услуги, който не е установен в Съюза, но предлага услуги в Съюза, определя писмено дадено юридическо или физическо лице за свой законен представител в Съюза за целите на получаването, спазването и изпълнението на заповеди за премахване, сигнали, искания и решения, издадени от компетентните органи на основание настоящия регламент. Законният представител пребивава или е установен в една от държавите членки, в които доставчикът на хостинг услуги предлага услугите си.

2. Доставчикът на хостинг услуги възлага на законния представител получаването, спазването и изпълнението на заповедите за премахване, сигналите, исканията и решенията, посочени в параграф 1, от името на въпросния доставчик на хостинг услуги. Доставчиците на хостинг услуги предоставят на своя законен представител необходимите правомощия и ресурси, за да си сътрудничат с компетентните органи и да спазват тези решения и заповеди.

3. Определеният законен представител може да бъде подведен под отговорност за неспазване на задълженията, произтичащи от настоящия регламент, без да се засягат отговорността на доставчика на хостинг услуги и правните действия, които могат да бъдат предприети срещу него.

4. Доставчикът на хостинг услуги уведомява компетентния орган, посочен в член 17, параграф 1, буква г), на държавата членка, в която пребивава или е установен законният представител относно определянето му. Информацията относно законният представител се прави обществено достояние.

РАЗДЕЛ VI
ЗАКЛЮЧИТЕЛНИ РАЗПОРЕДБИ

Член 17
Определяне на компетентните органи

1. Всяка държава членка определя органа или органите, които са компетентни:

   а) за издаването на заповеди за премахване в съответствие с член 4;

   б) за откриването и идентифицирането на терористично съдържание и за изпращането на сигнал за него до доставчиците на хостинг услуги в съответствие с член 5;

   в) за наблюдението на прилагането на проактивни мерки в съответствие с член 6;

   г) за налагането на принудително изпълнение на задълженията, произтичащи от настоящия регламент, посредством санкции в съответствие с член 18.

2. Най-късно до [*шест месеца след влизането в сила на настоящия регламент*] държавите членки уведомяват Комисията за компетентните органи, посочени в параграф 1. Комисията публикува уведомлението и всички негови изменения в *Официален вестник на Европейския съюз*.

Член 18
Санкции

1. Държавите членки установяват правилата относно санкциите, приложими при нарушения от страна на доставчиците на хостинг услуги на задълженията, произтичащи от настоящия регламент, и предприемат всички необходими мерки за гарантиране на тяхното налагане. Тези санкции се ограничават до нарушения на задълженията, произтичащи от:

   а) член 3, параграф 2 (условия за ползване на доставчиците на хостинг услуги);

   б) член 4, параграфи 2 и 6 (изпълнение на заповеди за премахване и обратна информация);

   в) член 5, параграфи 5 и 6 (оценка на сигнали и обратна информация);

   г) член 6, параграфи 2 и 4 (доклади за проактивните мерки и приемането на мерки след решение за налагане на конкретни проактивни мерки);

   д) член 7 (съхраняване на данни);

   е) член 8 (прозрачност);

   ж) член 9 (гаранции по отношение на проактивните мерки);

   з) член 10 (процедури за подаване на жалби);

и) член 11 (информация за доставчиците на съдържание);

й) член 13, параграф 4 (информация за доказателства за терористични престъпления);

к) член 14, параграф 1 (звена за контакт);

л) член 16 (определяне на законен представител).

2. Предвидените санкции трябва да бъдат ефективни, пропорционални и възпиращи. Най-късно до [*шест месеца от влизането в сила на настоящия регламент*] държавите членки съобщават на Комисията тези правила и мерки и ѝ съобщават незабавно всички последващи техни изменения

3. Държавите членки гарантират, че при определянето на вида и размера на санкциите компетентните органи вземат предвид всички значими обстоятелства, в това число:

а) естеството, тежестта и продължителността на нарушението;

б) дали нарушението е умишлено или е резултат от небрежност;

в) предишни нарушения, извършени от отговорното юридическо лице;

г) финансовата стабилност на отговорното юридическо лице;

д) степента на съдействие на доставчика на хостинг услуги с компетентните органи.

4. Държавите членки гарантират, че системното неспазване на задълженията по член 4, параграф 2 подлежи на финансови санкции в размер до 4 % от общия оборот на доставчика на хостинг услуги за последната финансова година.

Член 19

Технически изисквания и изменения на образците за заповедите за премахване

1. На Комисията се предоставя правомощието да приема делегирани актове в съответствие с член 20 с цел допълване на настоящия регламент с техническите изисквания за електронните средства, които да се използват от компетентните органи за връчването на заповедите за премахване.

2. На Комисията се предоставя правомощието да приема такива делегирани актове за изменение на приложения I, II и III с цел да се предприемат ефективни действия при евентуална необходимост от подобрения по отношение на съдържанието на формулярите за заповед за премахване и формулярите, които да се използват за предоставяне на информация относно невъзможността за изпълнение на заповед за премахване.

Член 20

Упражняване на делегирането

1. Правомощието да приема делегирани актове се предоставя на Комисията при спазване на предвидените в настоящия член условия.

2. Правомощието да приема делегирани актове, посочено в член 19, се предоставя на Комисията за неопределен срок, считано от [*датата на прилагане на настоящия регламент*].

3. Делегирането на правомощия, посочено в член 19, може да бъде оттеглено по всяко време от Европейския парламент или от Съвета. С решението за оттегляне се прекратява посоченото в него делегиране на правомощия. Оттеглянето поражда действие в деня след публикуването на решението в Официален вестник на Европейския съюз или на по-късна дата, посочена в решението. То не засяга действителността на делегираните актове, които вече са в сила.

4. Преди приемането на делегиран акт Комисията се консултира с експерти, определени от всяка държава членка в съответствие с принципите, залегнали в Междуинституционалното споразумение за по-добро законотворчество от 13 април 2016 година.

5. Веднага след като приеме делегиран акт, Комисията нотифицира акта едновременно на Европейския парламент и на Съвета.

6. Делегиран акт, приет съгласно член 19, влиза в сила единствено ако нито Европейският парламент, нито Съветът не са представили възражение в срок от два месеца след нотифицирането на същия акт на Европейския парламент и на Съвета, или ако преди изтичането на този срок и Европейският парламент, и Съветът са уведомили Комисията, че няма да представят възражения. Посоченият срок може да се удължи с два месеца по инициатива на Европейския парламент или на Съвета.

Член 21
Мониторинг

1. Държавите членки събират от своите компетентни органи и от доставчиците на хостинг услуги под тяхна юрисдикция информация за действията, които те са предприели в съответствие с настоящия регламенти, и я изпращат на Комисията всяка година до [31 март]. Тази информация включва:

   а) информация относно броя на издадените заповеди за премахване и подадените сигнали, броя на материалите с терористично съдържание, които са били премахнати или достъпът до които е бил блокиран, включително съответните срокове съгласно членове 4 и 5;

   б) информация относно конкретните проактивни мерки, предприети съгласно член 6, включително количеството терористично съдържание, което е било премахнато или достъпът до което е бил блокиран, и съответните срокове;

   в) информация относно броя на започнатите процедури за подаване на жалби и действията, предприети от доставчиците на хостинг услуги съгласно член 10;

   г) информация относно броя на започнатите процедури за правна защита и решенията, взети от компетентния орган в съответствие с националното законодателство.

2. Най-късно до [*една година от датата на прилагане на настоящия регламент*] Комисията изготвя подробна програма за мониторинг на крайните продукти, резултатите и въздействието на настоящия регламент. В програмата за мониторинг се определят показателите, средствата, чрез които се събират данните и другите необходими доказателства, и на какви интервали става това.

В нея се посочват действията, които да бъдат предприети от Комисията и от държавите членки при събирането и анализирането на данните и другите доказателства с оглед на мониторинга на напредъка и на оценката на настоящия регламент съгласно член 23.

Член 22
Доклад за изпълнение

Най-късно до [*две години след влизането в сила на настоящия регламент*] Комисията докладва на Европейския парламент и на Съвета относно прилагането на настоящия регламент. В доклада на Комисията се вземат предвид информацията относно мониторинга съгласно член 21 и информацията, произтичаща от задълженията за прозрачност съгласно член 8. Държавите членки предоставят на Комисията информацията, необходима за изготвянето на доклада.

Член 23
Оценка

Не по-рано от [*три години от датата на прилагане на настоящия регламент*] Комисията извършва оценка на настоящия регламент и представя доклад на Европейския парламент и на Съвета относно прилагането на настоящия регламент, включително ефективността на предпазните механизми. Когато това е целесъобразно, докладът се придружава от законодателни предложения. Държавите членки предоставят на Комисията информацията, необходима за изготвянето на доклада.

Член 24
Влизане в сила

Настоящият регламент влиза в сила на двадесетия ден след деня на публикуването му в *Официален вестник на Европейския съюз*.

Той се прилага от [6 месеца след влизането му в сила].

Настоящият регламент е задължителен в своята цялост и се прилага пряко във всички държави членки.

Съставено в Брюксел на […] година.

За Европейския парламент	*За Съвета*
Председател	*Председател*