ЕВРОПЕЙСКА
КОМИСИЯ

Брюксел, 14.2.2024 г.
COM(2024) 64 final

ДОКЛАД НА КОМИСИЯТА ДО ЕВРОПЕЙСКИЯ ПАРЛАМЕНТ И СЪВЕТА

относно прилагането на Регламент (ЕС) 2021/784 относно справянето с разпространението с терористично съдържание онлайн

{SWD(2024) 36 final}

1. РЕЗЮМЕ

Регламент (ЕС) 2021/784 относно справянето с разпространението на терористично съдържание онлайн осигурява на европейско равнище правната рамка, чрез която държавите членки защитават гражданите от излагане на терористични материали онлайн. Регламентът има за цел да гарантира безпрепятственото функциониране на цифровия единен пазар чрез справяне със злоупотребата с хостинг услуги за разпространение сред обществеността на терористично съдържание онлайн. Той има за цел да се предотврати използването на интернет от терористи, за да разпространяват посланията си с цел сплашване, радикализиране, вербуване и улесняване на терористични нападения. Това е особено важно в настоящия контекст на конфликти и нестабилност, които оказват влияние върху сигурността на Европа. Агресивната война на Русия срещу Украйна и терористичното нападение, извършено от Хамас срещу Израел на 7 октомври 2023 г., доведоха до увеличаване на разпространението на терористично съдържание онлайн.

Регулаторната рамка за справяне с незаконното съдържание онлайн беше допълнително укрепена с влизането в сила на 16 ноември 2022 г. на Законодателния акт за цифровите услуги. Законодателният акт за цифровите услуги урежда задълженията на доставчиците на цифрови услуги, които действат като посредници в ролята си да свързват потребителите със съдържание, услуги и стоки, като по този начин защитават по-добре ползвателите онлайн и допринасят за по-безопасна онлайн среда.

Регламентът относно справянето с разпространението на терористично съдържание онлайн влезе в сила на 7 юни 2022 г. Съгласно член 22 от Регламента Комисията представя на Европейския парламент и на Съвета доклад относно прилагането на Регламента („доклад за изпълнението“).

Настоящият доклад за изпълнението се основава на оценката на информацията, предоставена от държавите членки, Европол и доставчиците на хостинг услуги в съответствие със задълженията, установени в Регламента. Въз основа на тази оценка основните констатации относно прилагането на Регламента могат да бъдат обобщени, както следва:

- до 31 декември 2023 г. **двадесет и три държави членки** са определили компетентни органи с правомощието да издават заповеди за премахване, както е предвидено в Регламента[1]. Списъкът на органите на държавите членки е достъпен на уебсайта на Комисията и се актуализира редовно;[2]

- до 31 декември 2023 г. Комисията получи информация за най-малко **349 заповеди за премахване на терористично съдържание**, издадени от компетентните органи

[1] В онлайн регистъра, създаден от Комисията съгласно член 12, параграф 4 от Регламента, са изброени компетентните органи, посочени в член 12, параграф 1, и точката за контакт, определена или установена съгласно член 12, параграф 2, за всеки компетентен орган. Той се актуализира редовно въз основа на уведомленията, получени от държавите членки. Списък на националните компетентни органи и точки за контакт (europa.eu).

[2] Списък на националните компетентни органи и точки за контакт (europa.eu).

на шест държави членки (Испания, Румъния, Франция, Германия, Чехия и Австрия), които в повечето случаи са довели до бързи последващи действия от страна на доставчиците на хостинг услуги за премахване или блокиране на достъпа до терористично съдържание. Това доказва, че предвидените в Регламента инструменти започват да се използват и успешно гарантират бързото премахване на терористично съдържание от страна на доставчиците на хостинг услуги, както е предвидено в член 3, параграф 3. Според информацията, получена от Комисията, тези заповеди за премахване не са били оспорени;

- **координацията** при прилагането на Регламента, особено при обработването на заповеди за премахване на терористично съдържание, **работи добре** между компетентните органи на държавите членки и Европол, по-специално звеното на ЕС за сигнализиране за незаконно съдържание в интернет (EU IRU) към Европол.

- инструментът на Европол **PERCI**[3] е пуснат в действие на 3 юли 2023 г. Този инструмент се използва успешно от някои държави членки за предаване на заповеди за премахване и на сигнали[4]. Испанските, германските, австрийските, френските и чешките компетентни органи са използвали инструмента за предаването на заповеди за премахване на терористично съдържание. Като цяло през периода от стартирането на PERCI на 3 юли до 31 декември 2023 г. в PERCI са обработени най-малко 14 615 сигнала;

- в Регламента не се съдържат конкретни мерки по отношение на сигналите, но според информацията, получена от Комисията, след влизането му в сила се наблюдава също така **увеличаване на способността за реагиране на сигналите** от страна на доставчиците на хостинг услуги;

- въз основа на информацията, с която разполага Комисията, до 31 декември 2023 г. нито един доставчик на хостинг услуги не е бил счетен за изложен на терористично съдържание, както е определено в член 5, параграф 4 от Регламента. Установяването на този факт е предпоставка за прилагането на конкретните мерки, посочени в същия член. Според представените от доставчиците на хостинг услуги доклади за прозрачност обаче, те са предприели мерки **за справяне със злоупотребата с техните услуги** за разпространение на терористично съдържание, по-специално чрез приемането на специфични условия за ползване и прилагането на други разпоредби и мерки за ограничаване на разпространението на терористично съдържание;

- доставчиците на хостинг услуги също така са приели мерки за уведомяване **за непосредствена заплаха за живота** съгласно член 14, параграф 5 от Регламента.

[3] PERCI (*Plateforme Européenne de Retraits des Contenus illégaux sur Internet*) е платформа за премахване на незаконно съдържание онлайн, разработена и управлявана от Европол. Чрез платформата се подпомага прилагането на Регламента, като наред с други функционалности се предоставя техническо решение за обработване на сигнали и заповеди за премахване до доставчиците на хостинг услуги.

[4] Сигналите са механизъм за предупреждаване на доставчиците на хостинг услуги с цел доставчикът доброволно да разгледа съвместимостта на съдържанието със собствените му условия за ползване. В Регламента (съображение 40) се посочва, че сигналите са доказали своята ефективност и следва да останат на разположение в допълнение към заповедите за премахване.

По отношение на **по-малките доставчици на хостинг услуги** през 2021 г. Комисията обяви покана за представяне на предложения, за да ги подкрепи при прилагането на Регламента. През 2022 г. Комисията избра три проекта (вж. раздел 4.8.), като тяхното изпълнение започна през 2023 г. и вече са постигнати резултати в предоставянето на подкрепа на малките предприятия за спазване на Регламента.

На 26 януари 2023 г. Комисията започна производства за установяване на нарушения срещу 22 държави членки за това, че не са определили компетентни органи съгласно член 12, параграф 1 от Регламента и не са изпълнили задълженията си съгласно член 12, параграфи 2 и 3 и член 18, параграф 1, като изпрати **официални уведомителни писма**[5]. След започването на тези производства за установяване на нарушения се е увеличил броят на държавите членки, които уведомяват компетентните органи, отговарящи за обработването на заповеди за премахване, както е отразено в информацията, публикувана в онлайн регистъра[6]. Освен това до 21 декември 2023 г. са прекратени производствата по 11 от случаите, започнати през януари 2023 г.[7]

Въз основа на информацията, получена от държавите членки и Европол и предоставена от доставчиците на хостинг услуги, Комисията прецени, че прилагането на Регламента е оказало **положително въздействие** за ограничаване на разпространението на терористично съдържание онлайн.

2. КОНТЕКСТ

Регламентът започна да се прилага на 7 юни 2022 г. Той има за цел да гарантира безпрепятственото функциониране на цифровия единен пазар, чрез справяне със злоупотребата с хостинг услуги за разпространение сред обществеността на терористично съдържание онлайн. Регламентът предоставя на държавите членки целенасочени инструменти, под формата на заповеди за премахване на терористично съдържание, за справяне с разпространението на терористично съдържание онлайн и дава възможност на държавите членки да поискат от всички видове доставчици на хостинг услуги да предприемат конкретни мерки за защита на предоставяните от тях услуги от злоупотреба от страна на терористични субекти, ако бъдат изложени на терористично съдържание.

Освен това с влизането в сила на Законодателния акт за цифровите услуги на 16 ноември 2022 г. регулаторната среда се разширява с хоризонтално законодателство с широк обхват, насочено към гарантиране на по-безопасно цифрово пространство за потребителите, ефективни мерки за борба с незаконното съдържание и по-прозрачни условия на предоставянето на услугата. Законодателният акт за цифровите услуги предоставя на Комисията широки правомощия за надзор, разследване и правоприлагане, за да предприема действия, насочени към много големите онлайн платформи и търсачки. Тези действия

[5] Вж. съобщение за медиите: Терористично съдържание онлайн (europa.eu).
[6] Списък на националните компетентни органи и точки за контакт (europa.eu). В онлайн регистъра има информация за компетентните органи на 23 държави членки за издаване на заповеди за премахване съгласно член 12, параграф 1, буква а).
[7] Финландия, Малта, Чехия, Дания, Румъния, Швеция, Латвия, Испания, Литва, Австрия и Словакия.

включват искания за информация и разследвания на действията на дружествата за модериране на съдържание с възможност за налагане на глоби.

Законодателният акт за цифровите услуги дава възможност за справяне с всички форми на незаконно съдържание, което позволява на Комисията да поиска от платформите да предоставят данни, за да докажат, че изпълняват собствените си ангажименти за премахване на съдържание. Въпреки че Регламентът относно терористичното съдържание онлайн предоставя още по-мощен инструмент за тази специфична форма на незаконно съдържание, като съдържа правно задължение за премахване на съдържание в рамките на един час от получаването на заповед за премахване и ефективни механизми за санкциониране.

Както е подчертано от Европол в докладите за ситуацията и тенденциите при тероризма (TE-SAT)[8], публикувани през последните години, терористите използват активно интернет, за да разпространяват своите послания с цел сплашване, радикализиране, вербуване и улесняване на терористични нападения. Доброволните мерки и необвързващите препоръки допринасят за намаляване на наличието на терористично съдържание онлайн, но ограниченията, включително малкият брой доставчици на хостинг услуги, които приемат доброволни механизми[9], както и разпокъсаността на процедурните правила в държавите членки, ограничават ефективността и ефикасността на сътрудничеството между държавите членки и доставчиците на хостинг услуги и налагат въвеждането на регулаторни мерки[10]. Ето защо ефективното прилагане на Регламента е от ключово значение за справяне с разпространението на терористично съдържание онлайн. Комисията оказва активна подкрепа на националните компетентни органи в този процес.

Съгласно член 22 от Регламента до 7 юни 2023 г. Комисията трябваше да представи на Европейския парламент и на Съвета доклад относно прилагането на Регламента („доклад за изпълнението“), който се основава на информацията, предоставена от държавите членки, които от своя страна използват отчасти на информацията, предоставена от доставчиците на хостинг услуги (член 21). От една страна представянето на доклада за изпълнението беше забавено поради късното предаване на ключова информация на Комисията от държавите членки и доставчиците на хостинг услуги. От друга страна беше счетено за важно в доклада за изпълнението да се отрази използването на PERCI, която беше пусната в действие на 3 юли 2023 г. и оттогава се използва за обработването на заповеди за премахване съгласно Регламента.

Настоящият доклад за изпълнението има за цел единствено да се предостави фактически преглед на съответните въпроси, свързани с прилагането на Регламента. В него не се съдържат тълкувания на Регламента и не се изразява становище относно тълкувания или други мерки, предприети при прилагането на Регламента.

---

[8] TE-SAT на Европол за 2023 г. https://www.europol.europa.eu/cms/sites/default/files/documents/Europol_TE-SAT_2023.pdf и 2022 г. https://www.europol.europa.eu/cms/sites/default/files/documents/Tesat_Report_2022_0.pdf.

[9] Европейска комисия, (2018 г.) Оценка на въздействието, придружаваща предложението за Регламент относно предотвратяване на разпространението на терористично съдържание онлайн, SWD(2018) 408 final, посетено на 4.5.2023 г. на адрес: https://eur-lex.europa.eu/legal-content/BG/TXT/?uri=SWD%3A2018%3A408%3AFIN.

[10] Пак там.

В съответствие с член 21, параграф 2 от Регламента и до посочената дата (7 юни 2023 г.) Комисията трябваше да изготви подробна програма за мониторинг на резултатите и въздействието на Регламента. По-конкретно в програмата за мониторинг следва да бъдат определени показателите, средствата и интервалите, през които ще се събират данните и другите необходими доказателства. Тази програма е установена в придружаващия работен документ на службите на Комисията. 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 въздействието на Регламента и на извършването на оценка на Регламента съгласно член 23 от него.

3. ЦЕЛ И МЕТОДИКА НА ДОКЛАДА

Целта на настоящия доклад е да се извърши оценка на прилагането на Регламента и на неговото въздействие до момента за ограничаване на разпространението на терористично съдържание онлайн. Това включва действията, предприети от държавите членки и доставчиците на хостинг услуги, като например изменения на техните условия за ползване на услуги и насоки за общността, както и спазването от тяхна страна на заповедите за премахване и способността им за реагиране на тях.

За тази цел Комисията събра информация от държавите членки, звеното на Европол за сигнализиране за незаконно съдържание в интернет (EU IRU) към Европол и доставчиците на хостинг услуги, включително информация, съдържаща се в докладите за прозрачност и мониторинг съгласно членове 7, 8 и 21 от Регламента. 18 държави членки предоставиха информация съгласно членове 8 и 21. Информацията за действията, предприети от доставчиците на хостинг услуги, беше събрана посредством техните годишни доклади за прозрачност, Европол и чрез пряка доброволна комуникация със службите на Комисията. В настоящия доклад за изпълнение е включена информацията, получена от Комисията до 31 декември 2023 г.

Задължения за мониторинг и прозрачност (членове 21, 7 и 8)

Съгласно член 21, параграф 1 от Регламента, за изготвянето на доклада за изпълнението държавите членки са длъжни да събират информация от своите компетентни органи и от доставчиците на хостинг услуги под тяхна юрисдикция и да я изпращат на Комисията до 31 март всяка година. Това включва информация за действията, които са предприели в съответствие с регламента през предходната календарна година. В член 21, параграф 1 се посочва видът информация, която държавите членки следва да събират относно мерките, предприети за спазване на Регламента, като например подробна информация относно заповедите за премахване, броя на исканията за достъп до съхранявано съдържание, за да се даде възможност за провеждане на разследвания, процедури за подаване на жалби, административни и съдебни проверки.

В съответствие с член 7, параграф 1 от Регламента, доставчиците на хостинг услуги ясно установяват в своите условия за ползване политиката си за справяне с разпространението на терористично съдържание, включително, когато е целесъобразно, с подходящо обяснение за функционирането на конкретните мерки, включително, ако е приложимо, използването на автоматизирани инструменти.

Освен това съгласно член 7, параграф 2 от Регламента доставчик на хостинг услуги, който е предприел действия за справяне с разпространението на терористично съдържание или е бил задължен да предприеме действия съгласно Регламента през дадена календарна година, прави публично достъпен доклад за прозрачност относно предприетите през същата година действия. Този доклад следва да бъде публикуван преди 1 март на следващата година.

В член 7, параграф 3 от Регламента се определя минималната информация, която следва да бъде включена в тези доклади за прозрачност, като например предприетите мерки за идентифициране и блокиране на достъпа до терористично съдържание, броя на премахнатите и/или възстановените материали и резултатите от жалбите.

В съответствие с член 8 от Регламента определените компетентни органи на държавите членки публикуват годишни доклади за прозрачност за дейността си съгласно Регламента. В член 8, параграф 1 се посочва минималната информация, която следва да бъде включена в тези доклади[11].

До 31 декември 2023 г. осемнадесет държави членки изпратиха на Комисията информация за предприетите от тях действия в съответствие с Регламента, а двадесет и три държави членки са определили компетентни органи с правомощието да издават заповеди за премахване, както е предвидено в Регламента.

4. СПЕЦИФИЧНИ ЕЛЕМЕНТИ НА ОЦЕНЯВАНЕТО

4.1. ЗАПОВЕДИ ЗА ПРЕМАХВАНЕ (член 3)

До 31 декември 2023 г. Комисията беше информирана общо за най-малко 349 заповеди за премахване, изпратени до Telegram, Meta, Justpaste.it, TikTok, DATA ROOM S.R.L., FLOKINET S.R.L., Archive.org, Soundcloud, X, Jumpshare.com, Krakenfiles.com, Top4Top.net и Catbox от компетентните органи на Испания, Румъния, Франция, Германия, Австрия и Чехия.

Испанският компетентен орган — CITCO (*Centro de Inteligencia contra el Terrorismo y el Crimen Organizado*), е издал 62 заповеди за премахване, румънският компетентен орган (ANCOM — Autoritatea Națională pentru Administrare și Reglementare în Comunicații) е изпратил две, а френският компетентен орган (OCLCTIC — L'Office central de lutte contre la criminalité liée aux technologies de l'information et de la communication) — 26 заповеди за премахване. След терористичното нападение, извършено от Хамас срещу Израел, германският компетентен орган (BKA — Bundeskriminalamt) е изпратил 249 заповеди за премахване.

Испанският компетентен орган е издал 62 заповеди за премахване: осемнадесет преди стартирането на PERCI и четиридесет и четири след стартирането на PERCI. Той е предоставил подробно описание на предаването и последващите действия по първите издадени заповеди за премахване, което е от голямо значение за по-доброто разбиране на последиците и въздействието на Регламента.

[11] Вж. текста на Регламент (ЕС) 2021/784, член 8, параграф 1: https://eur-lex.europa.eu/legal-content/BG/TXT/HTML/?uri=CELEX:32021R0784.

Първите две заповеди за премахване бяха издадени от испанския компетентен орган на 24 април 2023 г.[12] Те са свързани с два материала с терористично съдържание, единият от които е свързан с десния тероризъм, а другият — с джихадизма. Съдържанието, за което е била издадена първата заповед за премахване, е документ в PDF формат, публикуван в Telegram с неограничен достъп, в който е имало пропаганда за терористично насилие и възхвала на десни терористични атаки. Терористичното съдържание, предмет на втората заповед за премахване, е видеоклип с изображения на джихадисти от така наречената терористична организация „Ислямска държава“ по време на бойни действия, което е било качено в Internet Archive. Тези два материала са били премахнати и от двете платформи за по-малко от един час, което е в съответствие с член 3, параграф 3 от Регламента. В оценката, предоставена от испанския компетентен орган, е обяснено, че вместо да подаде сигнал, той е решил да издаде заповед за премахване поради две основни причини: спазване на изискванията на Регламента относно заповедите за премахване и неотложност. Испанският компетентен орган след това издаде още заповеди за премахване:

Испанският орган подчерта предизвикателствата, свързани с използването от един от доставчиците на хостинг услуги (Meta) на уеб формуляр за получаването на заповеди за премахване, вместо да се предостави директна точка за контакт. Този уеб формуляр е довел и до проблеми при комуникацията с компетентния орган на държавата членка, в която е основното място на стопанска дейност на доставчика на хостинг услуги.

На 13 юли 2023 г. френският компетентен орган е издал първата си заповед за премахване до платформа за споделяне (Justpaste.it), която е премахнала терористичното съдържание в срок от един час. Съдържанието, към което е била насочена, е било пропаганда от „Ал Кайда“, по-точно от нейния медиен орган „Рикан Ка Мимбер“, от индийския клон на „Ал Кайда“ на Индийския субконтинент (AQIS). Пълното премахване на съдържанието беше потвърдено в платформата PERCI на Европол.

На 16, 18 и 24 октомври 2023 г. германският компетентен орган е издал съответно шест, шестнадесет и пет заповеди за премахване, които се отнасят до пропагандата на Хамас и движението „Ислямски джихад в Палестина“. В съответствие с член 3, параграф 3 от Регламента достъпът до съдържанието беше блокиран в ЕС. Германският компетентен орган първо е изпратил сигнали, но след като по тях не са били предприети действия, той е издал заповеди за премахване. След нападението на Хамас от 7 октомври германският компетентен орган е изпратил 249 заповеди за премахване, предимно до Telegram[13].

Чешкият компетентен орган и австрийският компетентен орган са издали съответно 2 и 8 заповеди за премахване, на X и Telegram.

Испанският компетентен орган е посочил два проблема във връзка с използването на уеб формуляр за получаването на заповеди за премахване от един доставчик на хостинг услуги: 1) в контекста на член 3, параграф 2 от Регламента наличието на уеб формуляр не позволява на компетентните органи на държавите членки да изпращат информация за приложимите процедури и срокове преди издаването на първата заповед за премахване до доставчика на хостинг услуги; 2) в контекста на член 4, параграф 1 наличието на уеб формуляр не

[12] Ministerio del Interior | El CITCO culmina la retirada de Internet de dos contenidos que alentaban al terrorismo.
[13] Според данните, с които разполага Комисията.

позволява да се изпрати копие от заповедта за премахване едновременно на компетентния орган на държавата членка, в която е основното място на стопанска дейност на доставчика на хостинг услуги, и на законния представител на доставчика на хостинг услуги.

4.2. ТРАНСГРАНИЧНИ ЗАПОВЕДИ ЗА ПРЕМАХВАНЕ (член 4)

Във връзка с двете първи заповеди за премахване, издадени през април 2023 г., испанският компетентен орган не е могъл да изпрати копия до органа на държавата членка, в която е било основното място на стопанска дейност на доставчика на хостинг услуги или неговият законен представител, тъй като по това време нито един от двамата доставчици на хостинг услуги не е имал основно място на стопанска дейност или определен законен представител в ЕС. Във връзка с последващите заповеди за премахване испанският компетентен орган е изпратил копия до компетентния орган на държавата членка, в която е било основното място на стопанска дейност на доставчика на хостинг услуги или в която той е определил свой законен представител.

Държавите членки докладват, че предаването на заповеди за премахване до установени в трети страни доставчици на хостинг услуги, които все още не са изпълнили задължението си да определят законен представител в ЕС, представлява предизвикателство. В този контекст и с цел да се осигурят незабавни действия Комисията оказа подкрепа на държавите членки, за да гарантират, че доставчиците на хостинг услуги изпълняват задължението си да определят законен представител в ЕС и да установят точка за контакт (член 15, параграф 1 от Регламента), като например адрес на електронна поща. Освен това Комисията е напомняла на доставчиците на хостинг услуги за задълженията им по време на различни форуми, включително в рамките на интернет форума на ЕС.

Според информацията, с която разполага Комисията, досега нито един компетентен орган на държавата членка, в която се намира основното място на стопанска дейност на доставчик на хостинг услуги, не е проверявал заповед за премахване съгласно член 4 от Регламента, за да прецени дали тя нарушава сериозно или явно Регламента или основните права и свободи, тъй като все още няма подадено нито едно мотивирано искане за проверка. В резултат на това досега нито един орган не е установил, че Регламентът или основните права са били нарушени от дадена заповед за премахване по този начин.

Досега нито един доставчик на хостинг услуги не е възстановил след проверка съгласно член 4 от Регламента съдържание (или достъпа до съдържание), което е било предмет на заповед за премахване, тъй като все още не са извършени такива проверки и няма искания за възстановяване. Поради това няма налична информация относно времето, което обикновено отнема възстановяването на съдържанието или на достъпа до него, както и за „необходимите мерки“, предприети от доставчиците на хостинг услуги, за да възстановят съдържанието или достъпа до него.

4.3. ПРАВНИ СРЕДСТВА ЗА ЗАЩИТА (член 9)

Според информацията, с която разполага Комисията, досега доставчиците на хостинг услуги не са оспорвали пред съответните съдилища заповеди за премахване или решения съгласно член 5, параграф 4. Един доставчик на хостинг услуги обаче твърди, че не е било възможно да изпълни заповед за премахване.

Според информацията, предоставена от държавите членки[14], най-малко дванадесет държави членки са въвели „ефективни процедури“, с които се дава възможност на доставчиците на хостинг услуги и доставчиците на съдържание да оспорят издадена заповед за премахване и/или решение, взето съгласно член 4, параграф 4 или член 5, параграфи 4, 6 или 7, пред съдилищата на компетентния орган на тези държави членки (член 9, параграфи 1 и 2). В държавите членки, в които са въведени такива процедури, те се отнасят предимно до съдебни производства. Въпреки това с настоящите данни, получени от държавите членки, не може да се установи дали тези процедури са „ефективни“ или специфични за Регламента, поради факта, че до момента няма оспорени решения.

4.4. КОНКРЕТНИ МЕРКИ И СВЪРЗАНА С ТЯХ ПРОЗРАЧНОСТ (членове 5 и 7)

Според наличната информация до този момент нито един доставчик на хостинг услуги не е счетен за изложен на терористично съдържание по смисъла на член 5, параграф 4 от Регламента. Поради това изискването за предприемане на конкретните мерки, посочени в същия член, (все още) не се прилага за нито един доставчик на хостинг услуги.

Според представените от доставчиците на хостинг услуги доклади за прозрачност обаче може да се отбележи, че няколко доставчици на хостинг услуги са предприели мерки за справяне със злоупотребата с техните услуги за разпространение на терористично съдържание, а именно приемането на специфични условия за ползване и прилагането на други разпоредби и мерки за ограничаване на разпространението на терористично съдържание. Както беше отбелязано по-горе, съгласно член 7 доставчиците на хостинг услуги трябва да осигурят прозрачност в това отношение не само чрез докладване за прозрачност, но и чрез включване на ясна информация в своите общи условия за ползване.

4.5. НЕПОСРЕДСТВЕНА ЗАПЛАХА ЗА ЖИВОТА (член 14, параграф 5)

В съответствие с член 14, параграф 5 от Регламента, когато доставчиците на хостинг услуги узнаят за терористично съдържание, сочещо непосредствена заплаха за живота, те незабавно информират органите, компетентни за разследването и наказателното преследване на престъпления в съответните държави членки. Когато не е възможно да се идентифицират съответните държави членки, доставчикът на хостинг услуги предава информацията на Европол с цел да бъдат предприети съответните последващи действия.

До 31 декември 2023 г. Комисията е била информирана за девет случая, в които звеното на ЕС за сигнализиране за незаконно съдържание в интернет към Европол е получило информация за терористично съдържание, включващо непосредствена заплаха за живота. Тъй като в член 14, параграф 5 от Регламента не се предвижда задължение за информиране на Европол във всички случаи, броят на уведомленията може да е по-голям. Испания е единствената държава членка, предоставила информация за прилагането на член 14, параграф 5. На 18 април 2023 г. испанските органи са получили съобщение от Amazon за предполагаемо терористично съдържание в платформата за видеоигри Twitch, сочещо непосредствена заплаха за живота.

[14] Следва да се отбележи, че предоставената информация не е непременно пълна. Необходими са допълнителни оценки, за да се получи цялостен и напълно актуален преглед на начина, по който държавите членки изпълняват изискването за осигуряване на наличието на ефективни процедури за правна защита.

Според оценката съдържанието не е отговаряло на условията за терористично съдържание, сочещо непосредствена заплаха за живота по смисъла на Регламента.

4.6. СЪТРУДНИЧЕСТВО МЕЖДУ ДОСТАВЧИЦИТЕ НА ХОСТИНГ УСЛУГИ, КОМПЕТЕНТНИТЕ ОРГАНИ И ЕВРОПОЛ (член 14)

Както е посочено по-горе, платформата „PERCI“ е разработена от Европол с цел да се подпомогне прилагането на Регламента чрез централизиране, координиране и улесняване на **предаването на заповеди за премахване и на сигнали** от държавите членки до доставчиците на хостинг услуги. Платформата функционира от 3 юли 2023 г. Преди пълното внедряване на PERCI, от Европол бяха въвели извънредни мерки с цел подпомагане на ръчното предаване на заповеди за премахване, избягване на конфликти в съдържанието, за да се избегне намеса в текущи разследвания, и реакция при кризи, свързани с „непосредствена заплаха за живота“.

PERCI е единна система, която дава възможност за сътрудничество между компетентните органи, доставчиците на хостинг услуги и Европол по отношение на въпросите в обхвата на Регламента, както е предвидено в член 14 от него. По-конкретно PERCI:

- е базирано в облак решение, предназначено да гарантира сигурността и защитата на данните в облака;
- е единна платформа за съвместна комуникация и координация в реално време, която подпомага бързото премахване на терористично съдържание;
- улеснява процеса на проверка на трансгранични заповеди за премахване;
- засилва избягването на конфликти, което е важно, за да се избегне възможността компетентният орган на дадена държава членка да изпрати заповед за премахване на съдържание, което е обект на текущо разследване в друга държава членка;
- дава възможност на доставчиците на хостинг услуги да получават заповеди за премахване по единен и стандартизиран начин от един канал.

Освен това PERCI дава възможност и за предаване на сигнали.

Понастоящем, освен че е от значение във връзка със сигналите (вж. съображение 40 от Регламента), PERCI улеснява предаването на заповеди за премахване (членове 3 и 4), докладването от страна на държавите членки (член 8) и координацията, както и избягването на конфликти в случай на противоречие с текущи разследвания относно съдържанието, за което е предвидено да се изпрати заповед за премахване (член 14). PERCI е в процес на допълнително разработване, за да може да подпомага допълнителни задачи, произтичащи от Регламента, като например проверка на трансгранични заповеди за премахване (член 4)[15].

[15] По-специално: — членове 3 и 4: предаване на заповеди за премахване; — член 3, параграфи 6—8: обратна информация от доставчиците на хостинг услуги; — член 4, параграфи 3—7: механизъм за проверка; — член 7: докладване: — член 14, параграф 1: избягване на конфликти, координация, избягване на дублиране; — член 14, параграф 3: сигурен канал за комуникация; — член 14, параграф 4: използване на специален инструмент, създаден от Европол; — член 14, параграф 5: съобщаване за „непосредствена заплаха за живота“; — съображение 40: предаване на сигнали.

Държавите членки потвърдиха, че съгласно член 14 от Регламента:

- компетентните органи обменят информация, координират се и си сътрудничат с други компетентни органи;
- компетентните органи обменят информация, координират се и си сътрудничат с Европол;
- съществуват механизми за подобряване на сътрудничеството, като същевременно се избягва намесата в разследвания, провеждани в други държави членки;
- повечето държави членки определят PERCI като предпочитан инструмент за предаване на заповеди за премахване, тъй като чрез него се постига координация на действията чрез избягване на конфликти.

4.7. ВЪЗДЕЙСТВИЕ ВЪРХУ СИГНАЛИТЕ

Сигнализирането за терористично съдържание е доброволен инструмент, който е бил използван и преди приемането на Регламента. Въпреки че в Регламента не се съдържат конкретни разпоредби по отношение на сигнализирането, в съответствие със съображение 40 в него не се изключва възможността държавите членки и Европол да използват сигнализирането като инструмент за справяне с терористично съдържание онлайн.

От създаването си през 2015 г. звеното на ЕС за сигнализиране за незаконно съдържание в интернет към Европол активно работи по идентифицирането на терористично съдържание онлайн и подаването на сигнали за него до доставчиците на хостинг услуги, както и по създаването на инструменти (т.е. PERCI, а преди това IRMA[16]) за улесняване на предаването на сигнали.

Според информацията, предоставена на Комисията, сигнализирането продължава да се използва от органите на държавите членки за определени доставчици на хостинг услуги, макар че те биха могли да разгледат възможността за издаване на заповеди за премахване до доставчици на хостинг услуги, които не предприемат действия по сигнали, или по други причини, като например спешна необходимост от премахване на съдържанието.

4.8. ПОДКРЕПА НА ПО-МАЛКИТЕ ДОСТАВЧИЦИ НА ХОСТИНГ УСЛУГИ ЗА ПРИЛАГАНЕТО НА РЕГЛАМЕНТА

В Регламента се съдържат различни задължения за доставчиците на хостинг услуги. Докато големите доставчици на хостинг услуги обикновено разполагат с необходимите технически възможности, кадрови капацитет за проверка и знания за прилагане на Регламента, малките доставчици на хостинг услуги може да разполагат с по-ограничени финансови, технически и човешки ресурси и експертен опит за тази цел. Същевременно по-малките доставчици на хостинг услуги все по-често стават обект на злонамерени участници, които се възползват от техните услуги. Това може да се дължи и на ефективните усилия за модериране на съдържание от страна на по-големите доставчици на хостинг услуги. Тази тенденция

[16] Приложението за управление на сигнализирането в интернет (IRMA) е създадено от Европол през 2016 г. с цел да се подпомогне подаването на сигнали за незаконно съдържание до доставчиците на онлайн услуги. Първоначално достъпът до IRMA е предоставен на служителите на Европол и на специализираните звена (IRU) в седем държави членки. От 3 юли 2023 г. PERCI замени IRMA.

показва успеха на мерките за модериране на съдържание, но тя също така подчертава необходимостта от подкрепа за по-малките доставчици на хостинг услуги, за да увеличат капацитета и знанията си с цел спазване на изискванията на Регламента.

В отговор на това предизвикателство Комисията отправи покана за представяне на предложения по линия на фонд „Вътрешна сигурност“ с цел да се окаже подкрепа на по-малките доставчици на хостинг услуги при прилагането на Регламента[17]. Комисията избра три проекта[18], за да ги подкрепи чрез подход в три направления. Първо, чрез информиране и повишаване на осведомеността относно разпоредбите и изискванията на Регламента, второ, чрез разработване, прилагане и въвеждане на инструменти и рамки, необходими за справяне с разпространението на терористично съдържание онлайн, и трето, чрез споделяне на опит и най-добри практики в сектора.

Работата по трите проекта започна през 2023 г. и вече са постигнати ценни резултати. Например в доклада за картографиране по проекта FRISCO[19] беше установено, че микро- и малките доставчици на хостинг услуги обикновено имат много ограничена осведоменост и познания за Регламента, и бяха подчертани потенциалните затруднения, с които биха могли да се сблъскат при предприемането на действия в отговор на заповеди за премахване в срок от един час, тъй като често не разполагат с услуги, които да се предоставят 24 часа в денонощието, 7 дни в седмицата. Липсата на ресурси е предизвикателство, както и създаването на линии за комуникация с правоприлагащите агенции. Повече от половината доставчици на хостинг услуги, анкетирани от изпълнителите, не модерират съдържание, създадено от потребителите, и са заявили, че никога не са попадали на терористично съдържание в своите платформи. Тези доставчици на хостинг услуги са склонни да предприемат ad hoc мерки, ако такова съдържание се появи на техните платформи.

Чрез тези три проекта малките доставчици на хостинг услуги получават подкрепа в усилията си да спазват разпоредбите на Регламента, като създават точки за контакт и прилагат механизми за подаване на жалби от ползвателите.

Освен това от значение по-специално за по-малките доставчици на хостинг услуги може да бъде член 3, параграф 2 от Регламента, съгласно който се изисква да се предоставя своевременно информация за приложимите процедури и срокове на доставчиците на хостинг услуги, на които не е била издадена предишна заповед за премахване.

---

[17] https://ec.europa.eu/info/funding-tenders/opportunities/docs/2021-2027/isf/wp-call/2021-2022/call-fiche_isf-2021-ag-tco_en.pdf.

[18] 1) Рамка за подпомагане на микро (и малки) доставчици на хостинг услуги при докладване и премахване на терористично съдържание онлайн, базирана на изкуствен интелект (ALLIES), 2) Борба с терористичното съдържание онлайн (FRISCO) и 3) Технология срещу тероризма в Европа (TATE). Връзка за повече информация: Финансиране и обществени поръчки (europa.eu).

[19] Проведено в рамките на шестмесечен период, приключил през май 2023 г. Докладът се основава на обратната информация от 48 европейски доставчици на хостинг услуги — 33 отговора чрез нашето онлайн проучване и 15 отговора чрез допитване. FRISCO, *D2.1: Доклад за картографиране на потребностите и пречките пред спазването на изискванията „Разбиране на потребностите и осведомеността на малките и микро- доставчици на хостинг услуги във връзка с прилагането на изискванията на Регламента за терористичното съдържание онлайн“*, достъпен на адрес Резултати | Frisco (friscoproject.eu).

4.9. ПРЕДПАЗНИ МЕРКИ ЗА ОСНОВНИТЕ ПРАВА

В Регламента са включени различни предпазни мерки за засилване на отчетността и прозрачността на предприетите мерки за премахване на терористично съдържание онлайн. В това отношение се прави препратка към изложеното по-горе, и по-специално към предоставената информация относно правните средства за защита, докладването и специалния механизъм за трансгранични заповеди за премахване.

Освен това в член 23 от Регламента се изисква Комисията да докладва за функционирането и ефективността на предпазните механизми, по-специално на предвидените в член 4, параграф 4, член 6, параграф 3 и членове 7—11 в контекста на оценката на Регламента. Такива предпазни мерки се отнасят до механизмите за подаване на жалби, правните средства за защита и санкциите, приети и прилагани срещу риска от погрешно премахване на терористично съдържание онлайн с цел защита на доставчиците на съдържание и на доставчиците на хостинг услуги. Следователно оценката на функционирането и ефективността на предпазните механизми ще бъде част от оценката съгласно член 23.

В тази връзка в програмата за мониторинг, посочена в член 21, параграф 2 от Регламента, е предвидена рамка от показатели за оценка на неговото въздействие върху основните права, която ще послужи за оценката на Регламента.

С програмата за мониторинг ще се подпомогне оценката, която ще бъде извършена като част от оценката на функционирането и ефективността на предпазните механизми, прилагани в контекста на Регламента, както и на тяхното въздействие върху основните права. Тази област на въздействие отразява двете области, посочени в член 23 от Регламента: а) функционирането и ефективността на предпазните механизми, по-специално на предвидените в член 4, параграф 4, член 6, параграф 3 и членове 7—11; и б) въздействието на прилагането на Регламента върху основните права, по-специално свободата на изразяване на мнение и свободата на информация, зачитането на личния живот и защитата на личните данни.

4.10. КОМПЕТЕНТНИ ОРГАНИ (член 13)

Съгласно член 13 от Регламента държавите членки трябва да гарантират, че техните компетентни органи разполагат с необходимите правомощия и с достатъчни ресурси за постигане на целите и за изпълнение на техните задълженията по Регламента. Някои държави членки са приложили следните мерки, за да гарантират, че компетентните органи разполагат с необходимите правомощия и с достатъчни ресурси:

- създаване на нови органи/дирекции;
- предоставяне на допълнително финансиране и допълнителен персонал и
- създаване на нови законодателни рамки.

5. ЗАКЛЮЧЕНИЕ

Изключително важно е всички инструменти и мерки на равнището на ЕС да бъдат изцяло приложени за бързо справяне с незаконното съдържание, разпространявано онлайн. Това е

особено вярно предвид огромния обем на това незаконно съдържание, както наскоро свидетелства разпространението на съдържание, свързано с нападението, извършено от Хамас срещу Израел.

Регламентът допринася за повишаване на обществената сигурност в целия Съюз, за да се предотврати използването от терористите на действащи на вътрешния пазар доставчици на хостинг услуги за разпространение на своите послания с цел сплашване, радикализиране, вербуване и улесняване на терористични нападения.

След започването на производствата за установяване на нарушения през януари 2023 г. **е постигнат напредък**. Както е отразено в онлайн регистъра, до 31 декември 2023 г. двадесет и три държави членки са определили компетентни органи съгласно член 12, параграф 1, което е довело до по-системно използване на мерките и инструментите, предвидени в Регламента. Освен това до 21 декември 2023 г. са били прекратени производствата по единадесет от двадесет и двата случая, започнати през януари 2023 г. Комисията настоятелно призовава останалите държави членки да предприемат необходимите стъпки, за да определят компетентните органи съгласно член 12, параграф 1 и да изпълнят задълженията си съгласно член 12, параграфи 2 и 3 и член 18, параграф 1.

Като цяло държавите членки докладват, че с подкрепата на Европол заповедите за премахване се предават безпроблемно на доставчиците на хостинг услуги. Въз основа на информацията, получена от държавите членки и Европол, от влизането в сила на Регламента са предадени най-малко 349 **заповеди за премахване на терористично съдържание**. В десет случая терористичното съдържание не е било премахнато/достъпът до него не е бил блокиран от един доставчик на хостинг услуги в рамките на установения в Регламента максимален срок от един час.

Според информацията, получена от държавите членки и Европол, способността за реагиране на сигнали за терористично съдържание се е увеличила след влизането в сила на Регламента, въпреки че в него не се съдържат разпоредби в това отношение. Освен това в съответствие с член 14, параграф 5 доставчиците на хостинг услуги са предали на Европол информация за терористично съдържание, включващо непосредствена заплаха за живота, в девет случая.

Налице са по-ефективни комуникационни канали и процедури, особено след стартирането на платформата PERCI на 3 юли 2023 г., което доведе до по-системен подход към предаването на заповеди за премахване, като същевременно PERCI се използва и за предаване на голям брой сигнали. Държавите членки и Европол изразиха очакване, че внедряването на PERCI ще допринесе за използването на тези инструменти за борба с терористичното съдържание онлайн.

Въз основа на това Комисията преценява, че като цяло Регламентът е оказал **положително въздействие** за ограничаване на разпространението на терористично съдържание онлайн. Въпреки това в десет от 349-те случая целевият доставчик на хостинг услуги е надхвърлил определения в Регламента максимален срок от един час за премахване на терористично съдържание или за блокиране на достъпа до него.

Комисията оказва активна подкрепа на държавите членки и на доставчиците на хостинг услуги, включително чрез технически семинари, организирани преди и след влизането в сила на Регламента. Последният семинар бе проведен на 24 ноември 2023 г. Комисията оказва подкрепа и на по-малките доставчици на хостинг услуги, за да гарантира пълното и бързо прилагане на Регламента, и им помага да се справят с предизвикателствата, с които са се сблъскали досега.

Комисията ще продължи да наблюдава изпълнението и прилагането на Регламента. Чрез програмата за мониторинг, която ще бъде включена в оценката на Регламента съгласно член 23, Комисията ще следи отблизо ефективността на предвидените в него инструменти.