ЕКЗД — ЕНОЗД

Съвместно становище 4/2022 относно предложението за регламент на Европейския парламент и на Съвета за определяне на правила за предотвратяване и борба със сексуалното насилие над деца

Прието на 28 юли 2022 г.

СЪДЪРЖАНИЕ

Общ преглед

На 11 май 2022 г. Европейската комисия публикува предложение за Регламент на Европейския парламент и на Съвета за определяне на правила за предотвратяване и борба със сексуалното насилие над деца.

В предложението се вменяват квалифицирани задължения на доставчиците на хостинг услуги, междуличностни съобщителни услуги и други услуги, във връзка с откриването, докладването, премахването и блокирането на известни и нови онлайн материали, съдържащи сексуално насилие над деца, както и установяването на контакт с деца. Предложението предвижда също създаването на нова, децентрализирана агенция на ЕС („Център на ЕС“) и мрежа от национални координационни органи по въпросите на сексуалното насилие над деца, с което да се даде възможност за прилагането на предложения регламент. Както е посочено в обяснителния меморандум към предложението, съдържащите се в предложението мерки могат да засегнат упражняването на основни права на ползвателите на въпросните услуги.

Сексуалното насилие над деца е особено тежко и ужасно престъпление и целта да се даде възможност за ефективни действия за борба с него представлява призната от Съюза цел от общ интерес и е насочена към защита на правата и свободите на жертвите. Същевременно ЕКЗД и ЕНОЗД припомнят, че всички ограничения на основните права, като например предвидените в предложението, трябва да отговарят на изискванията, посочени в член 52, параграф 1 от Хартата на основните права на Европейския съюз.

ЕКЗД и ЕНОЗД подчертават, че предложението поражда сериозни опасения относно пропорционалността на предвидената намеса и ограниченията върху защитата на основните права на неприкосновеност на личния живот и на защита на личните данни. В това отношение ЕКЗД и ЕНОЗД посочват, че процесуалните предпазни мерки никога не могат изцяло да заменят материалноправните такива. Въведената сложната система за предприемане на административните действия, от оценка на риска и мерки за намаляването му до издаването на заповед за откриване, не може да замени необходимата яснота на материалноправните задължения.

ЕКЗД и ЕНОЗД считат, че в предложението липсва яснота по ключови елементи, като например понятието „значителен риск“. Освен това субектите, които отговарят за прилагането на тези предпазни мерки, като се започне от частните оператори и се стигне до административните и/или съдебните органи, разполагат с много широка свобода на преценка, което води до правна несигурност по отношение на балансирането на разглежданите права във всеки отделен случай. ЕКЗД и ЕНОЗД подчертават, че когато се допуска особено сериозна намеса в основните права, законодателят трябва да осигури правна яснота относно това, кога и къде е разрешена намесата. Като изразяват съгласието си, че законодателството не може да бъде твърде регулирано и трябва да предвижда известна гъвкавост при практическото му прилагане, ЕКЗД и ЕНОЗД считат, че предложението оставя твърде много възможности за потенциални нарушения поради липсата на ясни материалноправни норми.

Що се отнася до необходимостта и пропорционалността на предвидените мерки за откриване, ЕКЗД и ЕНОЗД са особено загрижени по отношение на мерките, предвидени за откриването на неизвестни материали, съдържащи сексуално насилие над деца („СНД“) и установяването на контакт с деца („сприятеляване с деца“) с цел сексуална злоупотреба в междуличностните съобщителни услуги. Поради намесата при тези мерки, вероятностния им характер и процента на грешки, свързвани с тези

технологии, ЕКЗД и ЕНОЗД считат, че намесата в резултат на прилагането на такива мерки надхвърля необходимото и пропорционалното. Освен това мерките, които позволяват на публичните органи да имат общ достъп до съдържанието на дадено съобщение с цел откриване на случаи на установяване на контакт с деца е по-вероятно да засегнат същността на правата, гарантирани в членове 7 и 8 от Хартата. Поради това съответните разпоредби, свързани със сприятеляването с цел сексуална злоупотреба, следва да бъдат заличени от предложението. Освен това предложението не изключва от приложното си поле сканирането на звукови съобщения. ЕКЗД и ЕНОЗД считат, че сканирането на звукови съобщения е значителна намеса и като такава трябва да остане извън обхвата на задълженията за откриване, определени в предложения регламент, както по отношение на записи на гласови съобщения, така и по отношение на общуване в реално време.

ЕКЗД и ЕНОЗД също така изразяват съмнения относно ефективността на мерките за блокиране и считат, че изискването доставчиците на интернет услуги да декриптират онлайн съобщения, за да блокират такива, свързани със СНД, би било непропорционална мярка.

Освен това ЕКЗД и ЕНОЗД обръщат внимание на това, че технологиите за криптиране в основата си допринасят за зачитането на личната неприкосновеност и поверителния характер на съобщенията, свободата на изразяване на мнение, както и за иновациите и растежа на цифровата икономика, която разчита на високото равнище на доверие и сигурност, които тези технологии осигуряват. В съображение 26 от предложението се поставя условие по отношение не само на избора на технологии за откриване, но и на техническите мерки за защита на поверителността на съобщенията като криптиране, като се определя че този технологичен избор трябва да става при спазване на изискванията на предложения регламент, т.е. трябва да дава възможност за откриване. Това е в потвърждение на разбирането, което се внушава от член 8, параграф 3 и член 10, параграф 2 от предложението, че доставчик не може да откаже изпълнението на заповед за откриване на основание липса на техническа възможност. ЕКЗД и ЕНОЗД считат, че следва да има по-добро равновесие между обществената необходимост от сигурни и частни канали за комуникация и борбата срещу злоупотребата с тях. В предложението следва ясно да се посочи, че нищо в предложения регламент не следва да се тълкува в смисъл, че забранява или отслабва криптирането.

Въпреки че ЕКЗД и ЕНОЗД приветстват изявлението в предложението, в което се посочва, че то не засяга правомощията и компетенциите на органите в областта на защитата на данните съгласно ОРЗД, ЕКЗД и ЕНОЗД са на мнение, че връзката между задачите на координиращите органи и тези на органите по защита на данните следва все пак да бъде по-добре регламентирана. В това отношение ЕКЗД и ЕНОЗД признават ролята, която се възлага на ЕКЗД в предложението с изискването за участието му в практическото прилагане на предложението, по-специално необходимостта ЕКЗД да изготви становище относно технологиите, които Центърът на ЕС ще предоставя за изпълнението на заповедите за откриване. Следва обаче да се изясни каква е целта на становището в процеса и какви ще бъдат действията на Центъра на ЕС, след като получи становището на ЕКЗД.

И накрая, ЕКЗД и ЕНОЗД отбелязват, че предложението предвижда тясно сътрудничество между Центъра на ЕС и Европол, които следва да си предоставят взаимно „възможно най-пълен достъп до ... съответните информационни системи“. Въпреки че ЕКЗД и ЕНОЗД по принцип подкрепят сътрудничеството между двете агенции, предвид факта, че Центърът на ЕС не е правоприлагащ орган, все пак ЕКЗД и ЕНОЗД отправят няколко препоръки за подобряване на съответните разпоредби, включително че предаване на лични данни между Центъра на ЕС и Европол се извършва само в отделни индивидуални случаи, след старателна оценка на съответно искане и посредством инструмент за обмен на сигурна комуникация, като например мрежата SIENA.

Европейският комитет по защита на данните и Европейският надзорен орган по защита на данните,

като взеха предвид член 42, параграф 2 от Регламент (ЕС) 2018/1725 от 23 октомври 2018 г. относно защитата на физическите лица във връзка с обработването на лични данни от институциите, органите, службите и агенциите на Съюза и относно свободното движение на такива данни и за отмяна на Регламент (ЕО) № 45/2001 и Решение № 1247/2002/ЕО (РЗДЕС),[1]

като взеха предвид Споразумението за Европейското икономическо пространство, и по-конкретно приложение XI и протокол 37 към него, изменени с Решение на Съвместния комитет на ЕИП № 154/2018 от 6 юли 2018 г.,[2]

като взеха предвид искането на Европейската комисия от 12 май 2022 г. за съвместно становище на Европейския комитет по защита на данните и Европейския надзорен орган по защита на данните относно предложението за регламент на Европейския парламент и на Съвета за определяне на правила за предотвратяване и борба със сексуалното насилие над деца,[3]

ПРИЕХА СЛЕДНОТО СЪВМЕСТНО СТАНОВИЩЕ

1. ВЪВЕДЕНИЕ

1. На 11 май 2022 г. Европейската комисия („Комисията“) публикува предложение за Регламент на Европейския парламент и на Съвета за определяне на правила за предотвратяване и борба със сексуалното насилие над деца („предложението“ или „предложението за регламент“).[4]

2. Предложението беше направено след приемането на Регламент (ЕС) 2021/1232 относно временна дерогация от някои разпоредби на Директива 2002/58/ЕО по отношение на използването на технологии от доставчици на междуличностни съобщителни услуги без номерà за обработването на лични и други данни за целите на борбата с онлайн сексуалното насилие над деца („временния регламент“)[5]. Във временния регламент не се изисква от доставчиците на съответните услуги да въвеждат мерки за откриване на материали, съдържащи сексуално насилие над деца („СНД“) (напр. снимки, видеоклипове и др.) или установяване на контакт с деца (познато също като „сприятеляване с деца с цел сексуална злоупотреба“), но се позволява

[1] ОВ L 295, 21.11.2018 г., стр. 39.
[2] Позоваванията на държави членки в настоящия документ следва да се разбират като позовавания на държавите членки на ЕИП.
[3] Предложение за регламент на Европейския парламент и на Съвета за определяне на правила за предотвратяване и борба със сексуалното насилие над деца, COM (2022) 209 final.
[4] Пак там.
[5] Регламент (ЕС) 2021/1232 на Европейския парламент и на Съвета от 14 юли 2021 година относно временна дерогация от някои разпоредби на Директива 2002/58/ЕО по отношение на използването на технологии от доставчици на междуличностни съобщителни услуги без номерà за обработването на лични и други данни за целите на борбата с онлайн сексуалното насилие над деца (ОВ L 274, 2021 г., стр. 41).

на тези доставчици да правят това по собствена инициатива и в съответствие с условията, определени в посочения регламент.[6]

3. Предложението съдържа два основни градивни елемента. Най-напред се вменяват квалифицирани задължения на доставчиците на хостинг услуги, междуличностни съобщителни услуги и други услуги, във връзка с откриването, докладването, премахването и блокирането на известни и нови онлайн материали, съдържащи сексуално насилие над деца, както и установяването на контакт с деца. На второ място, в предложението се предвижда също създаването на нова, децентрализирана агенция на ЕС („Център на ЕС по въпросите на сексуалното насилие над деца“ или „Центъра на ЕС“) и мрежа от национални координационни органи по въпросите на сексуалното насилие над деца, с което да се даде възможност за прилагането на предложения регламент.[7]

4. Както е посочено в обяснителния меморандум към предложението, съдържащите се в предложението мерки могат да засегнат упражняването на основни права на ползвателите на въпросните услуги. Сред тези права могат да бъдат по-специално основните права на зачитане на неприкосновеността на личния живот (включително поверителността на съобщенията, като част от по-широкото право на зачитане на личния и семейния живот), защитата на личните данни и свободата на изразяване на мнение и на информация.[8]

5. Освен това така предложените мерки имат за цел доразвиването и в известна степен допълването на съществуващото законодателство на ЕС в областта на защитата на данните и неприкосновеността на личния живот. В това отношение в обяснителния меморандум се отбелязва, че:

> „Предложението се основава на Общия регламент относно защитата на данните (ОРЗД).” На практика доставчиците обикновено се позовават на различни основания за обработване, предвидени в ОРЗД, за да извършват обработването на лични данни, свързано с доброволното откриване и докладване на онлайн сексуално насилие над деца. С предложението се установява система от заповеди за целенасочено откриване и се определят условията за откриване, като се осигурява по-голяма правна сигурност за тези дейности. По отношение на задължителните дейности по откриване, включващи обработване на лични данни, с предложението, и по-специално с издадените въз основа на него заповеди, се създава основанието за такова обработване, както това е посочено в член 6, параграф 1, буква в) от ОРЗД, в който се предвижда обработване на лични данни, когато това е необходимо за спазването на законово задължение съгласно законодателството на Съюза или на държава членка, което се прилага спрямо администратора.
>
> Предложението обхваща, *inter alia*, доставчици, които предлагат междуличностни електронни съобщителни услуги и следователно са обект на националните разпоредби за прилагане на Директивата за правото на неприкосновеност на личния живот и електронни комуникации и на нейния предложен преработен вариант, който понастоящем се обсъжда. Предвидените в предложението мерки ограничават в някои

[6] Вж. също становище 7/2020 на ЕНОЗД относно предложението за временни дерогации от Директива 2002/58/ЕО за целите на борбата със сексуалното насилие над деца онлайн (10 ноември 2020 г.).
[7] COM(2022) 209 final, стр. 17.
[8] COM(2022) 209 final, стр. 12.

отношения обхвата на правата и задълженията съгласно съответните разпоредби на посочената директива, а именно във връзка с дейности, които са строго необходими за изпълнението на заповеди за откриване. Във връзка с това, предложението включва прилагането по аналогия на член 15, параграф 1 от посочената директива.“[9]

6. Предвид тежестта на предвидената намеса в основните права, предложението има особено значение за защитата на правата и свободите на физическите лица по отношение на обработването на лични данни. Поради това на 12 май 2022 г. Комисията реши да се консултира с Европейския комитет по защита на данните (ЕКЗД) и Европейския надзорен орган по защита на данните (ЕНОЗД) в съответствие с член 42, параграф 2 от РЗДЕС.

2. ПРИЛОЖНО ПОЛЕ НА СТАНОВИЩЕТО

7. Настоящото съвместно становище отразява общото мнение на ЕКЗД и ЕНОЗД по предложението. То е ограничено до аспектите на предложението, свързани със защитата на неприкосновеността на личния живот и личните данни. По-специално, в съвместното становище се посочват областите, в които предложението не осигурява достатъчна защита на основните права на неприкосновеност на личния живот и защита на данните, или е необходимо допълнително да бъде приведено в съответствие с правната рамка на ЕС в областта на защитата на неприкосновеността на личния живот и личните данни.

8. Както е обяснено допълнително в настоящото съвместно становище, предложението поражда сериозни опасения относно необходимостта и пропорционалността на предвидените намеси и ограниченията върху защитата на основните права на неприкосновеност на личния живот и на защита на личните данни. Целта на настоящото съвместно становище обаче не е да се предостави изчерпателен списък на всички проблеми, свързани с неприкосновеността на личния живот и защитата на данните, които поражда предложението, нито да се представят конкретни предложения за подобряване на формулировката му. По-скоро в настоящото съвместно становище са изложени обобщаващи бележки по основните въпроси, които поражда предложението, установени от ЕКЗД и ЕНОЗД. ЕКЗД и ЕНОЗД остават на разположение за предоставянето на съзаконодателите на допълнителни бележки и препоръки в хода на законодателния процес по предложението.

3. ОБЩИ БЕЛЕЖКИ ОТНОСНО ПРАВОТО НА ПОВЕРИТЕЛНОСТ НА КОМУНИКАЦИИТЕ И ПРАВОТО НА ЗАЩИТА НА ЛИЧНИТЕ ДАННИ

9. Поверителността на комуникациите е съществен елемент от основното право на зачитане на личния и семейния живот, залегнало в член 7 от Хартата на основните права на Европейския съюз („Хартата“).[10] Освен това в член 8 от Хартата се признава основното право на защита на личните данни. Правото на поверителност на комуникациите и правото на личен и семеен живот

[9] COM(2022) 209 final, стр. 4—5.
[10] Вж. напр. Становището на ЕКЗД относно преразглеждането на Регламента за неприкосновеността на личния живот в електронната среда и неговото въздействие върху защитата на физическите лица по отношение на неприкосновеността и поверителността на техните комуникации (25 май 2018 г.).

са гарантирани и в член 8 от Европейската конвенция за правата на човека („ЕКПЧ“) и са част от общите за държавите членки конституционни традиции.[11]

10. ЕКЗД и ЕНОЗД припомнят, че правата, залегнали в членове 7 и 8 от Хартата не представляват абсолютни права, а трябва да се разглеждат във връзка с функцията им в обществото.[12] Сексуалното насилие над деца е особено тежко и ужасно престъпление и целта да се даде възможност за ефективни действия за борба с него представлява призната от Съюза цел от общ интерес, насочена към защита на правата и свободите на жертвите. По отношение на ефективните действия за борба с престъпленията, извършени срещу малолетни и непълнолетни лица и други уязвими групи, Съдът на Европейския съюз („Съдът на ЕС“) подчертава, че позитивни задължения могат да произтичат от член 7 от Хартата, в който се задължават публичните органи да въведат правни мерки за защита на личния и семейния живот, жилището и комуникациите. Такива задължения могат да произтичат и от членове 3 и 4 от Хартата по отношение на защитата на физическата и психическата неприкосновеност на личността и забраната на изтезанията и на нечовешкото и унизително отношение.[13]

11. Същевременно всички ограничения на гарантираните от Хартата права като предвидените в предложението[14] трябва да отговарят на изискванията, посочени в член 52, параграф 1 от Хартата. Всяка мярка, която представлява намеса в правото на поверителност на комуникациите и правото на личен и семеен живот, трябва преди всичко да зачита същността на въпросните права.[15] Ако дадено право е изпразнено от основното си съдържание и частноправният субект не може да го упражни, това засяга самата същина на правото[16]. Намесата във връзка с преследваната цел не може да представлява такава непропорционална и непоносима намеса, накърняваща самата същина на гарантираното право.[17] Това означава, че дори основно право, което не е абсолютно по своя характер, като правото на поверителност на комуникациите и правото на защита на личните данни, има някои същински елементи, които не могат да бъдат ограничавани.

12. Съдът на ЕС многократно е прилагал критерия за „основното съдържание на дадено право“ по дела в областта на неприкосновеността на електронните комуникации. В решението по дело Tele2 Sverige и Watson Съдът постановява, че правна уредба, която не допуска запазване на съдържанието на съобщения, не засяга съществото съдържание на правата на

---

[11] В конституциите на почти всички европейски държави е включено правото на защита на поверителността на комуникациите. Вж. напр. член 15 от Конституцията на Република Италия, член 10 от Основния закон на Федерална република Германия, член 22 от Белгийската конституция и член 13 от Конституцията на Кралство Нидерландия.

[12] Вж., наред с другото, Решение на Съда на ЕС по Дело C-311/18, *Facebook Ireland u Schrems*, т. 172 и цитираната съдебна практика. Вж. също съображение 4 от ОРЗД.

[13] Съд на ЕС, Решение по Съединени дела C- 511/18, C- 512/18 и C- 520/18, La Quadrature du Net и др., т. 126—128. Вж. също Становище 7/2020 на ЕНОЗД относно предложението за временни дерогации от Директива 2002/58/ЕО за целите на борбата със сексуалното насилие над деца онлайн (10 ноември 2020 г.), т. 12.

[14] Вж. COM(2022) 209 final, стр. 12—13.

[15] Член 52, параграф 1 от Хартата.

[16] Вж. ЕНОЗД, Насоки за оценка на пропорционалността на мерките, които ограничават основните права на неприкосновеност на личния живот и на защита на личните данни (19 декември 2019 г.), стр. 8, налични на адрес https://edps.europa.eu/sites/default/files/publication/19-12-19_edps_proportionality_guidelines2_en.pdf.

[17] Съд на ЕС, Дело C-393/19, *ОМ*, т. 53.

неприкосновеност на личния живот и на защита на личните данни.[18] По делото Schrems Съдът на ЕС постановява, че правна уредба, осигуряваща общ достъп на публичните органи до съдържанието на електронни съобщения, трябва да се счита за засягаща съществото съдържание на основното право на зачитане на личния живот, гарантирано с член 7 от Хартата.[19] В решението по дело Digital Rights Ireland и Seitlinger и др., Съдът констатира, че макар запазването на данни, наложено от Директива 2006/24, да представлява особено тежка намеса в основното право на зачитане на личния живот и на останалите права, признати от член 7 от Хартата, тя не би могла да засегне съществото съдържание на тези права, доколкото споменатата директива не позволява да се разкрива самото съдържание на електронните съобщения[20]. От тази съдебна практика може да се направи заключението, че мерки, осигуряващи общ достъп на публичните органи до съдържанието на съобщения, е по-вероятно да засегнат съществото съдържание на правата, гарантирани в членове 7 и 8 от Хартата. Тези съображения са относими със същата сила и по отношение на мерки за откриване на СНД и установяване на контакт с деца като предвидените в предложението.

13. Освен това Съдът на ЕС констатира, че мерки за защита на сигурността на данните имат ключова роля за гарантиране, че няма да бъде засегнато съществото съдържание на основното право на защита на личните данни, признато в член 8 от Хартата.[21] В ерата на цифровите технологии техническите решения за гарантиране и защита на поверителността на електронните комуникации, включително мерки за криптиране, са от ключово значение за гарантиране на упражняването на всички основни права.[22] Това следва да бъде надлежно взето предвид при оценката на мерки за задължително откриване на СНД или установяване на контакт с деца, по-специално ако те биха довели до отслабване или влошаване на качеството на криптирането.[23]

14. Член 52, параграф 1 от Хартата предвижда също, че всяко ограничаване на упражняването на основно право, гарантирано от Хартата, трябва да бъде определено в закон. При спазване на принципа на пропорционалност ограничения могат да бъдат налагани, само ако са необходими и ако действително отговарят на признати от Съюза цели от общ интерес или на необходимостта да се защитят правата и свободите на други хора.[24] За да се изпълни изискването за пропорционалност, правната уредба трябва да предвижда ясни и точни правила, които определят обхвата и прилагането на въпросните мерки и налагат минимални предпазни мерки, така че лицата, чиито лични данни са засегнати да разполагат с достатъчни предпазни мерки, позволяващи ефикасна защита на тези данни срещу риск от злоупотреба.[25] В тази уредба трябва по-специално да се посочват обстоятелствата и условията, при които може да се приложи мярка, предвиждаща обработването на такива данни, като по този начин се гарантира ограничаване на

---

[18] Съд на ЕС, Съединени дела C-203/15 и C-698/15, Tele2 Sverige и Watson, т. 101.
[19] Съд на ЕС, Дело C-362/14, Schrems, т. 94.
[20] Съд на ЕС, Съединени дела C–293/12 и C–594/12, Digital Rights Ireland и Seitlinger и др., т. 39.
[21] Пак там, т. 40.
[22] Вж. Резолюция 47/16 на Съвета по правата на човека относно утвърждаването, защитата и упражняването на правата на човека в интернет, документ на ООН A/HRC//4/47(26 юли 2021 г.).
[23] Вж. също съображение 25 от временния регламент.
[24] Вж. „Оценка на необходимостта от мерки, ограничаващи основното право на защита на личните данни: инструментариум“, 11 април 2019 г., достъпен на адрес: https://edps.europa.eu/sites/default/files/publication/17-06-01_necessity_toolkit_final_en.pdf.
[25] Вж. Съд на ЕС, решение по Съединени дела C- 511/18, C- 512/18 и C- 520/18, La Quadrature du Net и др., т. 132.

намесата до строго необходимото.[26] Както пояснява Съдът на ЕС, необходимостта от такива предпазни мерки е още по-голяма, когато личните данни са подложени на автоматизирано обработване и най-вече, когато става дума за защита на чувствителни данни, които са особената категория лични данни.[27]

15. Предложението ще ограничи упражняването на правата и задълженията, предвидени в член 5, параграф 1, член 3 и член 6, параграф 1 от Директива 2002/58/ЕО („Директива за правото на неприкосновеност на личния живот и електронни комуникации“) [28] , доколкото това е необходимо за изпълнението на заповедите за откриване, издадени в съответствие с глава 1, раздел 2 от предложението. ЕКЗД и ЕНОЗД считат, че поради това е необходимо предложението да бъде оценявано не само с оглед на изискванията на Хартата и ОРЗД, но и с оглед на членове 5 и 6 и член 15, параграф 1 от Директивата за правото на неприкосновеност на личния живот и електронни комуникации.

[26] Пак там.
[27] Пак там.
[28] Директива 2002/58/ЕО на Европейския парламент и на Съвета от 12 юли 2002 година относно обработката на лични данни и защита на правото на неприкосновеност на личния живот в сектора на електронните комуникации („Директивата за правото на неприкосновеност на личния живот и електронни комуникации“), изменена с Директива 2006/24/ЕО и Директива 2009/136/ЕО.

4. КОНКРЕТНИ БЕЛЕЖКИ

4.1 Връзка със съществуващото законодателство

4.1.1 Връзка с ОРЗД и Директивата за правото на неприкосновеност на личния живот и електронни комуникации

16. В предложението се посочва, че то не засяга правилата, произтичащи от други актове на Съюза, по-специално ОРЗД [29] и Директивата за правото на неприкосновеност на личния живот и електронни комуникации. За разлика от временния регламент, предложението не предвижда изрична временна дерогация от упражняването на правата и задълженията, предвидени в член 5, параграфи 1 и 3 и член 6, параграф 1 от Директивата за правото на неприкосновеност на личния живот и електронни комуникации, а ограничаване на упражняването на тези права и задължения. Освен това следва да се отбележи, че временният регламент предвижда дерогация конкретно само от разпоредбите на член 5, параграф 1 и член 6, параграф 1, но не и от член 5, параграф 3 от Директивата за правото на неприкосновеност на личния живот и електронни комуникации.

17. Освен това предложението се позовава на член 15, параграф 1 от Директивата за правото на неприкосновеност на личния живот и електронни комуникации, който допуска държавите членки да приемат законодателни мерки за ограничаване на обхвата на правата и задълженията, предвидени в членове 5 и 6 от посочената директива, когато такова ограничаване представлява необходима, подходяща и пропорционална мярка в рамките на демократично общество, inter alia, за предотвратяването, разследването, разкриването и наказателното преследване на криминални престъпления. Съгласно предложението, член 15, параграф 1 от Директивата за правото на неприкосновеност на личния живот и електронни комуникации се прилага по аналогия, когато е предвидено ограничаване на упражняването на правата и задълженията, предвидени в член 5, параграфи 1 и 3 и член 6, параграф 1 от Директивата за правото на неприкосновеност на личния живот и електронни комуникации.

18. ЕКЗД и ЕНОЗД припомнят, че Съдът на ЕС ясно е определил, че член 15, параграф 1 от Директивата за правото на неприкосновеност на личния живот и електронни комуникации следва да се тълкува стриктно, което означава, че изключението от принципа на поверителност на комуникациите, което член 15, параграф 1 допуска, трябва да остане изключение и да не се превръща в правило.[30] Както е посочено по-нататък в настоящото съвместно становище, ЕКЗД и ЕНОЗД считат, че предложението не отговаря на изискванията за (строго) необходими, ефективни и пропорционални мерки. Освен това, ЕКЗД и ЕНОЗД стигат до заключението, че предложението може да доведе до това намесата в поверителността на комуникациите да се превърне по същество в правило, вместо да остане изключение.

[29] Регламент (ЕС) 2016/679 на Европейския парламент и на Съвета от 27 април 2016 г. относно защитата на физическите лица във връзка с обработването на лични данни и относно свободното движение на такива данни и за отмяна на Директива 95/46/ЕО (Общ регламент относно защитата на данните) (текст от значение за ЕИП) (ОВ L 119, 4.5.2016 г., стр. 1—88).

[30] Решение на Съда на ЕС от 21 декември 2016 г. по Съединени дела C-203/15 и C-698/15, Tele2 Sverige AB и Watson, т. 89.

4.1.2 Връзка с Регламент (ЕС) 2021/1232 и въздействие върху откриване по собствена инициатива на онлайн сексуално насилие над деца

19. Съгласно член 88 от предложението последното ще отмени временния регламент, който предвижда временна дерогация от някои разпоредби на Директивата за правото на неприкосновеност на личния живот и електронни комуникации, за да се даде възможност за използване по собствена инициатива от доставчици на междуличностни съобщителни услуги без номерà на технологии за откриване на СНД и случаи на установяване на контакт с деца. Следователно, от датата на прилагане на предложения регламент няма да има дерогация от Директивата за правото на неприкосновеност на личния живот и електронни комуникации, която да позволява откриване по собствена инициатива от такива доставчици на онлайн сексуално насилие над деца.

20. Като се има предвид, че задълженията за откриване, въведени с предложението, ще се прилагат само за получатели на заповеди за откриване, важно е в текста на предложения регламент да се поясни, че използването по собствена инициатива на технологии за откриване на СНД и установяване на контакт с деца с цел сексуална злоупотреба продължава да е разрешено само доколкото това се допуска съгласно Директивата за правото на неприкосновеност на личния живот и електронни комуникации и ОРЗД. Това би означавало например, че доставчиците на междуличностни съобщителни услуги без номерà няма да могат да използват такива технологии по собствена инициатива, освен ако това не е разрешено съгласно националните закони за транспониране на Директивата за правото на неприкосновеност на личния живот и електронни комуникации, в съответствие с член 15, параграф 1 от Директивата за правото на неприкосновеност на личния живот и електронни комуникации и Хартата.

21. В по-общ план, за предложения регламент ще е от полза допълнителното изясняване по отношение на правния статут на откриването по собствена инициатива на онлайн сексуално насилие над деца след датата на прилагане на предложения регламент, както и по отношение на преминаването от режим на откриване по собствена инициатива, така както той е предвиден във временния регламент, към задълженията за откриване, определени в предложения регламент. Например, ЕКЗД и ЕНОЗД препоръчват да се поясни, че предложеният регламент не предоставя правно основание за обработването на лични данни единствено с цел откриване по собствена инициатива на онлайн сексуално насилие над деца.

4.2 Правно основание съгласно ОРЗД

22. Предложението има за цел да създаде правно основание по смисъла на ОРЗД за обработването на лични данни за целите на откриване на СНД и сприятеляване с деца с цел сексуална злоупотреба. Съответно в обяснителния меморандум се отбелязва: „По отношение на задължителните дейности по откриване, включващи обработване на лични данни, с предложението, и по-специално с издадените въз основа на него заповеди, се създава основанието за такова обработване, посочено в член 6, параграф 1, буква в) от ОРЗД, който предвижда обработването на лични данни, необходимо за спазването на законово задължение съгласно законодателството на Съюза или на държава членка, което се прилага спрямо администратора“.[31]

[31] Пак там, стр. 4.

23. ЕКЗД и ЕНОЗД приветстват решението на Комисията да премахне правната несигурност по отношение на правното основание за обработването на лични данни, която се създава с временния регламент. ЕКЗД и ЕНОЗД са съгласни и със заключението на Комисията, че последствията от въвеждането на мерки за откриване са твърде широкообхватни и сериозни, за да се остави на доставчиците на услуги да вземат решението дали да приложат такива мерки.[32] Същевременно, ЕКЗД и ЕНОЗД отбелязват, че всяко правно основание, определящо задължения за доставчиците на услуги да се намесват в основните права в областта на защитата на данните и неприкосновеността на личния живот, ще има правно действие само доколкото в него са спазени условията, определени в член 52, параграф 1 от Хартата, както това е анализирано в следващите раздели.

4.3 Задължения за оценка и намаляване на риска

24. Съгласно глава II, раздел 1 от предложението от доставчиците на хостинг услуги и доставчиците на междуличностни съобщителни услуги се изисква да установяват, анализират и оценяват за всяка такава услуга, която предлагат, риска услугата да бъде използвана за целите на онлайн сексуално насилие над деца, след което да се стараят да сведат до минимум установения риск чрез прилагане на „разумни мерки за намаляване на риска, съобразени с установения … риск“.

25. ЕКЗД и ЕНОЗД отбелязват, че при извършването на оценка на риска доставчикът следва да вземе предвид по-специално елементите, изброени в член 3, параграф 2, букви а) — д) от предложението, включително: забрани и ограничения, предвидени в общите условия на договорите на доставчика; начина, по който ползвателите използват услугата, и неговото въздействие върху този риск; начина, по който доставчикът е проектирал и експлоатира услугата, включително модела на стопанска дейност, управлението и съответните системи и процеси, както и тяхното въздействие върху този риск. По отношение на риска от установяване на контакт с деца със сексуална цел, предложените елементи, които следва да бъдат взети предвид, са: степента, в която услугата се използва или има вероятност да се използва от деца; възрастовите групи и риска от установяване на контакт във връзка с тези възрастови групи; наличието на функционалности, създаващи възможност ползвателите да извършват търсене на други потребители, функционалности, създаващи възможност ползвателите да установяват контакт директно с други потребители, по-специално чрез лични съобщения, и функционалности, създаващи възможност ползвателите да споделят изображения или видеоклипове с други ползватели.

26. Въпреки че ЕКЗД и ЕНОЗД са съгласни, че тези критерии изглеждат уместни, все пак изразяват загриженост, че подобни критерии предоставят доста широка свобода на тълкуване и преценка. Няколко от критериите са описани с много общи понятия (напр. „начина, по който ползвателите използват услугата, и неговото въздействие върху този риск„) или са свързани с основни функционални възможности, които са обичайни за много онлайн услуги (напр. „възможност ползвателите да споделят изображения или видеоклипове с други ползватели“). В този си вид критериите могат лесно да станат предмет на субективна (а не обективна) преценка.

27. Според ЕКЗД и ЕНОЗД същото може да се каже и за мерките за намаляване на риска, които трябва да бъдат предприети съгласно член 4 от предложението. Мерки като адаптиране, чрез подходящи технически и оперативни мерки и персонал, на системите на доставчика за модериране или препоръчване на съдържание изглеждат подходящи за намаляване на

[32] Вж. предложението, COM(2022) 209 final, стр. 14.

установения риск. Когато обаче се прилагат в рамките на процес за комплексна оценка на риска и се съчетават с абстрактни и неясни понятия за описване на допустимата степен на риска (напр. „в значителна степен“), тези критерии не отговарят на изискванията за правна сигурност и предвидимост, необходими за обосноваване на намеса в поверителността на комуникациите между частни лица, която представлява категорична намеса в основните права на неприкосновеност на личния живот и свобода на изразяване на мнение.

28. Въпреки че доставчиците нямат право да се намесват в поверителността на комуникациите като част от своите стратегии за оценка и намаляване на риска преди получаване на заповед за откриване, налице е пряка връзка между оценката на риска и задълженията за намаляването му, и произтичащите от тях задължения за откриване. Съгласно член 7, параграф 4 от предложението издаването на заповед за откриване е поставено в зависимост от наличието на доказателства за значителен риск, че съответната услуга може да бъде използвана за целите на онлайн сексуално насилие над деца. Преди да бъде издадена заповед за откриване трябва да се спази сложен процес с участието на доставчиците, координиращият орган и съдебен или друг независим административен орган, компетентен за издаването на заповедта. Най-напред доставчиците трябва да направят оценка на риска услугите им да бъдат използвани за целите на онлайн сексуално насилие над деца (член 3 от предложението) и да анализират възможните мерки за намаляване (член 4 от предложението) с цел намаляване на този риск. След това резултатите от тази дейност се докладват на компетентния координиращ орган (член 5 от предложението). Ако оценката на риска показва, че въпреки усилията за намаляване на риска продължава да съществува значителен риск, координиращият орган изслушва доставчика относно изготвянето на проект на искане за издаване на заповед за откриване и му дава възможност да представи коментари. Освен това, доставчикът е длъжен да представи план за изпълнение, включително становище от компетентния орган по защита на данните, в случай на откриване на сприятеляване с деца с цел сексуална злоупотреба. Ако координиращият орган продължи с хода на процедурата по случая, се иска издаване на заповед за откриване, която впоследствие се издава от съд или друг независим административен орган. Поради това първоначалната оценка на риска и избраните мерки за намаляване на установения риск са решаващи и основа за оценката от страна на координиращия орган, както и на компетентния съдебен или административен орган, дали е необходима заповед за откриване.

29. ЕКЗД и ЕНОЗД отбелязват сложните етапи, водещи до издаването на заповед за откриване, които включват първоначална оценка на риска от доставчика и предложение на доставчика за мерки за намаляване на риска, както и по-нататъшно взаимодействие на доставчика с компетентния координиращ орган. ЕКЗД и ЕНОЗД считат, че съществува значителна възможност доставчикът да повлияе на резултата от процеса. Във връзка с това ЕКЗД и ЕНОЗД отбелязват, че в съображение 17 от предложението се посочва, че доставчиците следва да могат да посочват като част от докладването за риска „своето желание и готовност“ евентуално да им бъде издадена заповед за откриване. Поради това не може да се приеме, че всеки един доставчик ще се стреми да избегне да му бъде издадена заповед за откриване, за да защити поверителността на комуникациите на своите ползватели, чрез прилагане на най-ефективните мерки за намаляване на риска, които са с най-малка намеса, особено когато тези мерки за намаляване засягат свободата на доставчика да извършва стопанска дейност в съответствие с член 16 от Хартата.

30. ЕНОЗД и ЕКЗД биха искали да подчертаят, че процесуалните предпазни мерки никога не могат изцяло да заменят материалноправните. Поради това описаният по-горе сложен процес, водещ до евентуално издаване на заповед за откриване, следва да бъде придружен от ясни

материалноправни задължения. ЕКЗД и ЕНОЗД считат, че в предложението липсва яснота по няколко ключови елемента (напр. понятията „значителен риск“, „значителна степен“ и т.н.), което не може да бъде компенсирано от наличието на процесуални предпазни мерки на множество нива. Това е от още по-голямо значение с оглед на обстоятелството, че субектите, които отговарят за прилагането на тези предпазни мерки (напр. доставчици, съдебни органи и др.), разполагат с широка свобода на преценката за това как да се намери равновесието спрямо засегнатите права във всеки отделен случай. С оглед на значителната намеса в основните права, която би произтекла от приемането на предложението, законодателят следва да гарантира, че предложението предоставя повече яснота по отношение на това кога и къде е разрешена подобна намеса. Като се съгласяват, че законодателните мерки не могат да бъдат прекалено регулиращи и трябва да позволяват известна гъвкавост при практическото им прилагане, ЕКЗД и ЕНОЗД считат, че настоящият текст на предложението оставя твърде много възможности за потенциални злоупотреби поради липсата на ясни материалноправни норми.

31. Предвид потенциалното значително въздействие върху много голям брой субекти на данни (т.е. потенциално всички ползватели на междуличностни съобщителни услуги), ЕКЗД и ЕНОЗД подчертават необходимостта от висока степен на правна сигурност, яснота и предвидимост на законодателството, за да се гарантира, че предложените мерки действително са ефективни за постигането на преследваната с тях цел и същевременно възможно най-малко в ущърб на засегнатите основни права.

4.4 Условия за издаване на заповеди за откриване

32. В член 7 от предложението се предвижда, че координиращият орган по място на стопанска дейност има правомощието да поиска от компетентния съдебен орган на държавата членка, която го е определила, или от друг независим административен орган на тази държава членка, да издаде заповед за откриване, с която се изисква доставчик на хостинг услуги или доставчик на междуличностни съобщителни услуги да предприеме мерките, посочени в член 10, за откриване на онлайн сексуално насилие над деца в конкретна услуга.

33. ЕКЗД и ЕНОЗД надлежно вземат предвид следните елементи, които трябва да бъдат изпълнени преди издаването на заповед за откриване:

    а. налице са доказателства за значителен риск услугата да бъде използвана за целите на онлайн сексуално насилие над деца по смисъла на член 7, параграфи 5, 6 или 7, според случая;

    б. основанията за издаване на заповедта за откриване надделяват по значение над отрицателните последици за правата и законните интереси на всички засегнати страни, като се има предвид, по-специално, необходимостта да се осигури справедлив баланс между основните права на тези страни.

34. Значението на „значителен риск“ е определено в член 7, параграф 5 и по-нататък, в зависимост от вида на заповедта за откриване, която се разглежда. По отношение на заповеди за откриване, отнасящи се до откриването на известни материали, съдържащи СНД, значителен риск е налице, когато:

    а. въпреки всички мерки за намаляване на риска, които доставчикът може да е предприел или ще предприеме, съществува вероятност услугата да се използва в значителна степен за разпространението на известни материали, съдържащи сексуално насилие над деца; и

б. има доказателства, че услугата — или подобна услуга, в случай, че към датата на искането за издаване на заповед за откриване подобна услуга все още не се предлага в Съюза — е била използвана през последните 12 месеца в значителна степен за разпространение на известни материали, съдържащи сексуално насилие над деца.

35. За да се издаде заповед за откриване на нови материали, съдържащи СНД, вероятността и фактическите доказателства трябва да се отнасят до нови материали, съдържащи СНД, както и да е била издадена заповед за откриване на известни материали, съдържащи СНД и доставчикът да е представил значителен брой доклади относно материали със СНД, (член 7, параграф 6 от предложението). По отношение на заповеди за откриване, отнасящи се до установяване на контакт с деца с цел сексуална злоупотреба се счита, че значителен риск е налице, когато доставчикът се определя като доставчик на междуличностни съобщителни услуги, има вероятност услугата да се използва в значителна степен за установяване на контакт с деца и има доказателства, че услугата е била използвана в значителна степен за установяване на контакт с деца (член 7, параграф 7 от предложението).

36. ЕКЗД и ЕНОЗД отбелязват, че дори при критериите, определени в член 7, параграфи 5—7 от предложението, в условията за издаване на заповед за откриване преобладават някои неясни правни понятия като „значителна степен“ и „значителен брой“ и тези условия са отчасти повтарящи се, тъй като доказателствата за предишна злоупотреба често са основа за установяване на вероятността от бъдеща злоупотреба.

37. В предложението се предвижда система, при която, когато се решава дали е необходима заповед за откриване, трябва да се вземе прогнозно решение относно използването в бъдеще на дадена услуга за целите на онлайн сексуално насилие над деца. Поради това е разбираемо, че елементите, посочени в член 7, имат прогнозен характер. Използването на неясни понятия в предложението обаче затруднява доставчиците, както и компетентния съдебен или друг независим административен орган, оправомощен да прилага въведените с предложението правни изисквания по предвидим и непроизволен начин. ЕКЗД и ЕНОЗД са загрижени, че тези широки и неясни понятия ще доведат до липса на правна сигурност и също така до значителни различия в конкретното прилагане на предложението в рамките на Съюза, в зависимост от тълкуванията, които ще бъдат дадени на понятия като „вероятност“ и „значителна степен“ от съдебни или други независими административни органи в държавите членки. Такъв резултат би бил неприемлив с оглед на факта, че разпоредбите относно издаването на заповеди за откриване към доставчиците на междуличностни съобщителни услуги представляват „ограничаване“ на принципа на поверителност на комуникациите, установен в член 5 от Директивата за правото на неприкосновеност на личния живот и електронни комуникации, и следователно тяхната яснота и предвидимост са от изключително значение, за да се гарантира, че това ограничаване се прилага по еднакъв начин в целия Съюз.

4.5 Анализ на необходимостта и пропорционалността на предвидените мерки[33]

38. Както е посочено по-горе, съществуват три вида заповеди за откриване, които могат да бъдат издадени: заповеди за откриване, отнасящи се до разпространението на известни материали, показващи сексуално насилие над деца (член 7, параграф 5 от предложението), заповеди за откриване, отнасящи се до разпространението на нови материали, съдържащи сексуално

[33] Вж. също „Кратко ръководство на ЕНОЗД относно необходимостта и пропорционалността“, достъпно на адрес: https://edps.europa.eu/sites/default/files/publication/20-01-28_edps_quickguide_en.pdf.

насилие над деца (член 7, параграф 6 от предложението), и заповеди за откриване, отнасящи се до установяване на контакт с деца за сексуални цели (член 7, параграф 7 от предложението). За практическото изпълнение на всяка заповед за откриване обикновено е необходима различна технология. Следователно е налице различна степен на намеса, а оттук и различно въздействие върху правото на неприкосновеност на личния живот и защитата на личните данни.

39. Технологиите за откриване на материали, за които е известно, че съдържат сексуално насилие над деца, обикновено са технологии за намиране на съответствия, в смисъл че те разчитат на съществуваща база данни с известни материали със СНД, с която могат да се сравняват изображения (включително стоп кадри от видео материали). За да се даде възможност за съпоставяне, изображенията, които доставчикът обработва, както и изображенията в базата данни трябва да са в цифров вид, което обикновено се извършва чрез преобразуването им в хеш стойности. При този вид технология за хеширане процентът на фалшивите положителни съвпадения се оценява на не повече от 1 на всеки 50 милиарда (т.е. 0,000000002 % фалшиво положително съпоставяне). [34]

40. За откриването на нови материали със СНД обикновено се използва различен вид технология, включително класификатори и изкуствен интелект (ИИ). [35] Техният процент на грешка обаче като цяло е значително по-висок. Например в доклада за оценка на въздействието се посочва, че съществуват технологии за откриване на нови материали със СНД, чиято степен на точност може да бъде зададена на 99,9 % (т.е. 0,1 % фалшиво положително съпоставяне), но с тази степен на точност с тях е възможно да се установят едва 80 % от общия брой материали със СНД в съответния набор от данни. [36]

41. Що се отнася до откриването на случаи на контакт с деца със сексуална цел в текстови съобщения, в доклада за оценка на въздействието се пояснява, че това обикновено се основава на откриване на модели. В доклада за оценка на въздействието се отбелязва, че някои от съществуващите технологии за откриване на сприятеляване с деца с цел сексуална злоупотреба са с „точност“ от 88 %[37]. Според Комисията това означава, че „от 100 разговора, отбелязани като вероятен престъпен контакт с деца със сексуална цел, 12 могат да бъдат изключени при проверката [съгласно предложението — от Центъра на ЕС] и няма да бъдат докладвани на правоприлагащите органи“. [38] Но въпреки че — за разлика от временния регламент — предложението ще се прилага и за звуковите комуникации, в доклада за оценка на въздействието не се разглеждат подробно технологичните решения, които биха могли да се използват за откриване на сприятеляване с деца с цел сексуална злоупотреба в такава среда.

---

[34] Вж. Европейска комисия, Работен документ на службите на Комисията, Доклад за оценка на въздействието, придружаващ документа „Предложение за регламент на Европейския парламент и на Съвета за определяне на правила за предотвратяване и борба със сексуалното насилие над деца „„ SWD(2022) 209 final (наричан по-долу „Доклад за оценка на въздействието“ или „SWD(2022) 209 final“), стр. 281, fn. 511.

[35] Доклад за оценка на въздействието, стр. 281.

[36] Пак там, стр. 282.

[37] Пак там, стр. 283.

[38] Предложение, COM(2022) 209 final, стр. 14. fn. 32.

4.5.1 Ефективност на откриването

42. Необходима е основана на факти оценка на ефективността на предвидените мерки за постигането на преследваната цел и на това дали те са с по-слаба намеса в сравнение с други възможни решения за постигането на същата цел.[39] Друг фактор, който трябва да се вземе предвид при оценката на пропорционалността на дадена предложена мярка, е ефективността на съществуващите мерки в допълнение към предложената мярка.[40] Ако вече съществуват мерки за постигането на същата или подобна цел, следва да бъде направена оценка на тяхната ефективност като част от оценката на пропорционалността. Без такава оценка на ефективността на съществуващите мерки, преследващи същата или подобна цел, проверката за пропорционалност за дадена нова мярка не може да се счита за надлежно извършена.

43. Откриването от доставчици на хостинг услуги и доставчици на междуличностни съобщителни услуги на материали със СНД или на случаи на сприятеляване с деца с цел сексуална злоупотреба може да допринесе за постигането на общата цел за предотвратяване и борба със сексуалното насилие над деца и онлайн разпространението на материали, съдържащи сексуално насилие над деца. Същевременно необходимостта от оценка на ефективността на мерките, предвидени в предложението, поражда три ключови въпроса:

- Могат ли мерките за откриване на онлайн сексуално насилие над деца лесно да бъдат заобиколени?
- Какво ще бъде въздействието на дейностите по откриване върху действията, предприемани от правоприлагащите органи?[41]
- Как предложението би намалило правната несигурност?

44. Не е задача на ЕКЗД и ЕНОЗД да отговорят изчерпателно на тези въпроси. ЕКЗД и ЕНОЗД обаче отбелязват, че те не са разгледани изцяло нито в доклада за оценка на въздействието, нито в предложението.

45. Що се отнася до възможността за заобикаляне на задължението за откриване на СНД следва да се отбележи, че понастоящем изглежда не съществува технологично решение за откриване на СНД, споделяно в криптирана форма. Поради това всяка дейност по откриване — дори сканиране за действия от страна на клиента с цел заобикаляне на предлаганото от доставчика цялостно криптиране на комуникацията[42] — може лесно да бъде заобиколена чрез криптиране на съдържанието с помощта на отделно приложение преди изпращането или качването му. По този начин мерките за откриване, предвидени в предложението, може да имат по-слабо въздействие върху разпространението на СНД в интернет, отколкото може да се очаква.

---

[39] ЕНОЗД, „Оценка на необходимостта от мерки, ограничаващи основното право на защита на личните данни: инструментариум (11 април 2017 г., стр. 5; ЕНОЗД, Насоки на ЕНОЗД за оценка на пропорционалността на мерки, които ограничават основните права на неприкосновеност на личния живот и на защита на личните данни (19 декември 2019 г.), стр. 8.

[40] ЕНОЗД, Насоки на ЕНОЗД за оценка на пропорционалността на мерки, които ограничават основните права на неприкосновеност на личния живот и на защита на личните данни (19 декември 2019 г.), стр. 11.

[41] Според доклада за оценка на въздействието, приложение II, стр. 132, 85,71 % от респондентите в проучване сред правоприлагащите органи са изразили своята загриженост във връзка с увеличения брой материали, съдържащи сексуално насилие над деца през последното десетилетие, и липсата на ресурси (т.е. човешки, технически).

[42] Вж. също раздел 4.10 по-долу.

46. Също така Комисията очаква увеличаване на броя на докладите за сексуално насилие над деца до правоприлагащите органи с въвеждането на задълженията за откриване, предвидени с предложението [43] . Въпреки това нито в предложението, нито в доклада за оценка на въздействието се обяснява как това ще елиминира недостатъците при настоящото положение. Предвид ограничените ресурси на правоприлагащите органи, изглежда е необходимо да се обясни по-добре дали увеличаването на броя на докладите би имало някакво значимо въздействие върху правоприлагащите дейности срещу сексуалното насилие над деца. Във всеки случай ЕКЗД и ЕНОЗД биха искали да подчертаят, че тези доклади следва да бъдат оценявани своевременно, за да се гарантира, че решението относно наказателноправната значимост на докладваните материали ще бъде взето на възможно най-ранен етап и да се ограничи, доколкото е възможно, съхраняването на неотносими данни.

4.5.2 Възможно най-малка степен на намеса

47. Ако се допусне, че е възможно да бъдат реализирани положителните ефекти от откриването на СНД и сприятеляване с деца с цел сексуална злоупотреба, както това се предвижда от Комисията, мярката по откриване трябва да бъде с най-малка степен на намеса от всички мерки със същата ефективност. В член 4 от предложението се предвижда, че като първа стъпка доставчиците следва да обмислят предприемането на мерки за намаляване на риска техните услуги да бъдат използвани за целите на онлайн сексуалното насилие над деца под прага, който дава основание за издаване на заповед за откриване. Ако съществуват мерки за ограничаване на риска, които биха могли да доведат до значително намаляване на обменените съобщения за сприятеляване с деца с цел сексуална злоупотреба или СНД в рамките на съответната услуга, тези мерки най-често са с по-ниска степен на намеса в сравнение със заповедта за разкриване.[44] Поради това, ако съответният доставчик не предприеме такива мерки по собствена инициатива, следва да бъде предвидена възможност компетентният независим административен или съдебен орган да въведе задължение за прилагането на мерки за намаляване на риска и да осигури неговото изпълнение, вместо да издава заповед за откриване. Според ЕКЗД и ЕНОЗД фактът, че в член 5, параграф 4 от предложението се дава възможност на координиращия орган да „изисква“ от доставчика да въведе, преразгледа, прекрати или разшири мерките за намаляване на риска, не е достатъчен, тъй като такова изискване не би било самостоятелно приложимо; неизпълнението му ще се „санкционира“ само чрез издаване на заповед за откриване.

48. Поради това ЕКЗД и ЕНОЗД считат, че координиращият орган или компетентният независим административен или съдебен орган следва да бъдат изрично оправомощени да налагат мерки за смекчаване на риска, които са с по-слаба намеса, преди или вместо издаването на заповед за откриване.

[43] Вж., *inter alia*, Доклад за оценка на въздействието, приложение 3, SWD (2022) 209 final, стр. 176.

[44] Например биха могли да се обмислят мерки като блокиране от страна на клиентите на предаването на съобщения, съдържащи СНД, чрез предотвратяване на качването и изпращането на съдържание на електронните съобщения, тъй като такива мерки могат да помогнат в определен случай да се предотврати разпространението на известни материали, съдържащи СНД.

4.5.3 Пропорционалност в тесен смисъл

49. За да бъде една мярка съобразена с принципа на пропорционалност, залегнал в член 52, параграф 1 от Хартата, предимствата, произтичащи от мярката, следва да не бъдат неутрализирани от неблагоприятните последици, които тя създава по отношение на упражняването на основните права. Следователно принципът на пропорционалност „ограничава органите при упражняването на техните правомощия, като изисква да се постигне баланс между използваните средства и преследваната цел (или постигнатия резултат)“.[45]

50. За да може да се оцени въздействието на дадена мярка върху основните права на неприкосновеност на личния живот и на защита на личните данни, е особено важно точно да се определят:[46]

- **мащабите на мярката**, включително броят на засегнатите лица и дали тя води до „съпътстваща намеса“ (т.е. намеса в неприкосновеността на личния живот на лица, различни от тези, по отношение на които се прилага мярката);
- **обхватът на мярката**, включително количеството събрана информация; продължителността; дали разглежданата мярка изисква събирането и обработването на специални категории данни;
- **степента на намеса**, предвид естеството на дейността, предмет на мярката (дали засяга дейности, обхванати от задължението за поверителност или не, отношения между адвокат и клиент; медицинска дейност); контекстът; дали е равнозначна на профилиране на засегнатите лица или не; дали обработването предполага използването (частично или изцяло) на автоматизирана система за вземане на решения с „допустима грешка“;
- дали се отнася до **уязвими лица**;
- дали засяга и **други основни права** (например правото на свобода на изразяване на мнение, както в делата *Digital Rights Ireland u Seitlinger* и др. и *Tele2 Sverige u Watson*).[47]

51. В тази връзка е важно също така да се отбележи, че въздействието може да е незначително по отношение на засегнатото лице, но въпреки това да е значително или от изключителна колективна важност/за обществото като цяло.[48]

52. И в трите вида заповеди за откриване (откриване на известни материали, съдържащи СНД, нови материали, съдържащи СНД, и сприятеляване с деца с цел сексуална злоупотреба) наличните

---

[45] Вж. Дело C-343/09, *Afton Chemical*, т. 45; Съединени дела C-92/09 и C-93/09, *Volker und Markus Schecke u Hartmut Eifert*, т. 74; Дела C-581/10 и C-629/10, *Nelson u др.*, т. 71; Дело C-283/11, *Sky Österreich*, т. 50; и Дело C-101/12, *Schaible*, т. 29. Вж. също ЕНОЗД, „Оценка на необходимостта от мерки, ограничаващи основното право на защита на личните данни: инструментариум (11 април 2017 г.).

[46] ЕНОЗД, „Насоки за оценка на пропорционалността на мерките, които ограничават основните права на неприкосновеност на личния живот и на защита на личните данни“ (19 декември 2019 г.), стр. 23.

[47] Вж. също Становище 7/2020 на ЕНОЗД относно предложението за временни дерогации от Директива 2002/58/ЕО за целите на борбата със сексуалното насилие над деца онлайн (10 ноември 2020 г.), стр. 9 и следващите.

[48] ЕНОЗД, „Насоки за оценка на пропорционалността на мерките, които ограничават основните права на неприкосновеност на личния живот и на защита на личните данни“ (19 декември 2019 г.), стр. 20.

понастоящем технологии се основават на автоматизираното обработване на данни от съдържанието на всички засегнати потребители. Технологиите, използвани за анализ на съдържание, често са сложни и обикновено включват използването на ИИ. В резултат на това поведението на тази технология може да не е напълно разбираемо за ползвателя на услугата. Освен това се знае, че наличните понастоящем технологии, особено тези за откриване на нови материали, съдържащи СНД, или на случаи на сприятеляване с деца с цел сексуална злоупотреба, имат относително висок процент на грешки.[49] Също така съществува риск да бъде докладвано на Центъра на ЕС в съответствие с член 12, параграф 1 и член 48, параграф 1 от предложението, въз основа на открито „потенциално" СНД.

53. Освен това общите условия за издаване на заповед за откриване съгласно предложението, т.е. прилагани за цялата услуга, а не само за избрани съобщения[50], продължителността до 24 месеца за известни или нови случаи на СНД и до 12 месеца за сприятеляване с деца с цел сексуална злоупотреба[51] и т.н. могат практически да доведат до много широк обхват на заповедта. В резултат на това наблюдението всъщност ще бъде общо и неизбирателно по своя характер и на практика няма да бъде целенасочено.

54. С оглед на гореизложеното ЕКЗД и ЕНОЗД са загрижени също относно възможния възпиращ ефект върху упражняването на свободата на изразяване на мнение. ЕКЗД и ЕНОЗД припомнят, че такъв възпиращ ефект се счита за по-вероятен, когато законодателството е по-неясно.

55. При липсата на конкретизиране, прецизност и яснота, необходими за удовлетворяване на изискването за правна сигурност, [52] и като се има предвид широкият обхват, т.е. всички доставчици на съответни услуги на информационното общество, предлагащи такива услуги в Съюза,[53] предложението не гарантира, че по същество ще се осъществява само целенасочен подход към СНД и установяването на сприятеляване с деца с цел сексуална злоупотреба. Поради това ЕКЗД и ЕНОЗД считат, че на практика предложението би могло да се превърне в основа за *de facto* повсеместно и неизбирателно сканиране за проверка на съдържанието на буквално всички видове електронни комуникации на всички потребители в ЕС/ЕИП. В резултат на това законодателството може да накара хората да се въздържат от споделяне на законосъобразно съдържание поради опасения, че могат да станат мишена на правни действия въз основа на действията си.

56. Въпреки това, ЕКЗД и ЕНОЗД са съгласни, че различните мерки за борба със онлайн сексуалното насилие над деца може да включват различни степени на намеса. Като предварителен коментар ЕКЗД и ЕНОЗД отбелязват, че автоматизираният анализ на реч или текст с цел установяване на потенциални случаи на склоняване на деца с цел сексуална злоупотреба може да представлява по-значителна намеса от съпоставянето на изображения или видеоматериали въз основа на предварително потвърдени случаи на СНД с цел откриване на разпространение на материали, съдържащи СНД. Освен това следва да се прави разграничение между откриването на „известни материали, съдържащи СНД" и на „нови материали, съдържащи СНД". Също така въздействието следва да бъде допълнително разграничено между мерките, насочени към доставчиците на хостинг услуги, и мерките, налагани на доставчиците на междуличностни съобщителни услуги.

---

[49] Вж. подробности по-горе в т. 4.5 и по-долу, подточка 4.8.2.
[50] Вж. член 7, параграф 1 от предложението.
[51] Вж. член 7, параграф 9, трета алинея от предложението.
[52] Вж. Съд на ЕС, Дело C-197/96, Комисия на Европейските общности/Френска република, т. 15.
[53] Вж. член 1, параграф 2 от предложението.

4.5.4 Откриване на известни материали, съдържащи сексуално насилие над деца

57. Въпреки че съгласно съображение 4 предложението е „технологично неутрално“, ефективността на предложените мерки за откриване, както и тяхното въздействие върху отделните лица ще зависят до голяма степен от избора на прилаганата технология и от избраните индикатори. Този факт се признава от Комисията в приложение 8 към доклада за оценка на въздействието[54] и се потвърждава от други проучвания, като например целевата заместваща оценка на въздействието от февруари 2021 г. на Службата на ЕП за парламентарни изследвания относно предложението на Комисията за временна дерогация от Директивата за правото на неприкосновеност на личния живот и електронни комуникации за целите на борбата с онлайн сексуалното насилие над деца.[55]

58. В член 10 от предложението се определят редица изисквания към технологиите, които трябва да се използват за целите на откриването, по-специално по отношение на тяхната ефективност, надеждност и най-слаба намеса по отношение на въздействието върху правата на личен и семеен живот, включително на поверителност на съобщенията, както и на защитата на личните данни на ползвателите.

59. В този смисъл ЕКЗД и ЕНОЗД отбелязват, че понастоящем единствените технологии, които изглежда могат да отговорят като цяло на тези стандарти, са тези, които се използват за откриване на познати случаи на СНД, т.е. технологии за намиране на съответствия, които се основават на сравнителна база данни с хеш кодове.

4.5.5 Откриване на неизвестни до момента материали, съдържащи сексуално насилие над деца

60. Оценката на мерките, насочени към откриване на непознати до момента (нови) материали със СНД, води до различни заключения относно тяхната ефективност, надеждност и ограничаване на въздействието върху основните права на неприкосновеност на личния живот и защита на данните.

61. На първо място, както е обяснено в доклада за оценка на въздействието към предложението, използваните понастоящем технологии за откриване на неизвестни до момента материали, съдържащи СНД, включват класификатори и ИИ. Класификатор е всеки алгоритъм, който сортира данните в етикетирани класове или категории информация чрез разпознаване на модели.[56] Така тези технологии са с различни резултати и въздействие по отношение на точността, ефективността и степента на намеса. В същото време те са по-податливи на грешки.

62. Техниките, използвани за откриване на непознати до момента материали, съдържащи СНД, са сходни с тези, използвани за откриване на случаи на установяване на контакт с деца с цел сексуална злоупотреба, тъй като и двете се основават не на обикновени технологии за намиране

---

[54] Вж. информация за процента на фалшивите положителни резултати в доклада за оценка на въздействието, приложение 8, стр. 279 и следващите.

[55] Вж. предложение на Комисията за временна дерогация от Директивата за правото на неприкосновеност на личния живот и електронни комуникации за целите на борбата с онлайн сексуалното насилие над деца: целева заместваща оценка на въздействието (Служба на ЕП за парламентарни изследвания, февруари 2021 г.), стр. 14 и следващите.

[56] Доклад за оценка на въздействието, приложение 8, стр. 281.

на съответствия, а на прогнозни модели с използване на технологии с ИИ. ЕКЗД и ЕНОЗД считат, че следва да се подхожда с висока степен на предпазливост при откриване на непознати до момента материали, съдържащи СНД, тъй като една грешка в системата може да има тежки последици за субектите на данни, за които автоматично ще бъде отчетено, че е вероятно да са извършили много тежко престъпление и ще бъдат докладвани личните им данни и подробна информация за техните комуникации.

63. На второ място показателите за ефективност, установени в писмени източници, върху някои от които е поставен акцент в доклада за оценка на въздействието, придружаващ предложението,[57] предоставят много малко информация относно условията, които са използвани за тяхното изчисляване и за тяхната адекватност спрямо реалните условия, което означава, че тяхната ефективност в реални условия може да е значително по-ниска от очакваното, което води до занижена точност и по-висок процент на „фалшиви положителни резултати“.

64. На трето място показателите за ефективност следва да се разглеждат в специфичния контекст на използване на съответните инструменти за откриване и да предоставят изчерпателна информация за поведението на инструментите за откриване. Налице е достатъчно документална информация, че когато се използват алгоритми с изкуствен интелект за изображения или текст, може да се получи изместване и дискриминиране поради липсата на представителност на определени групи от населението в данните, използвани за обучението на алгоритъма. Тези отклонения следва да бъдат установени, измерени и намалени до приемливо равнище, за да могат системите за откриване да бъдат наистина полезни за обществото като цяло.

65. Въпреки че е направено проучване на технологиите, използвани за откриване,[58] ЕКЗД и ЕНОЗД считат, че е необходим допълнителен анализ, за да се оцени надеждността на съществуващите инструменти. Този анализ следва да се основава на изчерпателни индикатори за ефективността и да дава оценка на въздействието на потенциалните грешки в реални условия върху всички субекти на данни, засегнати от предложението.

66. Както беше отбелязано по-горе, ЕКЗД и ЕНОЗД имат сериозни съмнения по отношение на това до каква степен процедурните предпазни мерки, предвидени в член 7, параграф 6 от предложението, са достатъчни за компенсиране на тези рискове. Освен това те отбелязват, както беше посочено и по-горе, че в предложението се използват доста абстрактни и неясни понятия за описанието на допустимия риск (напр. „значителна степен“).

67. ЕКЗД и ЕНОЗД имат опасения, че тези широки и неясни понятия ще доведат до липса на правна сигурност и също така ще станат причина за големи различия при конкретното прилагане на предложението в рамките на Съюза, в зависимост от тълкуванията, които ще бъдат дадени на понятия като „вероятност“ и „значителна степен“ от съдебни или други независими административни органи в държавите членки. Това буди тревога също с оглед на факта, че разпоредбите относно заповедите за откриване ще представляват „ограничаване“ на принципа на поверителност, установен в член 5 от Директивата за правото на неприкосновеност на личния живот и електронни комуникации. Поради това е необходимо тяхната яснота и предвидимост да бъдат подобрени в предложения регламент.

[57] Доклад за оценка на въздействието, приложение 8, стр. 281—283.
[58] Доклад за оценка на въздействието, стр. 279 и сл.

4.5.6 Откриване на случаи на установяване на контакт с деца („сприятеляване“) с цел сексуална злоупотреба

68. ЕКЗД и ЕНОЗД отбелязват, че предложените мерки относно откриването на случаи на установяване на контакт („сприятеляване“) с деца с цел сексуална злоупотреба, които предполагат автоматизиран анализ на реч или текст, вероятно ще представляват най-значителната намеса в правата на личен и семеен живот, включително на поверителност на комуникациите и на защита на личните данни на ползвателите.

69. Въпреки че откриването на известни и дори на нови материали, съдържащи СНД, може да бъде ограничено по обхват до анализа на изображения и видеоматериали, откриването на сприятеляване с цел сексуална злоупотреба по дефиниция би трябвало да обхваща всички текстови (и евентуално звукови) съобщения, които попадат в обхвата на заповедта за откриване. В резултат на това степента на намеса в поверителността на съответните комуникации е много по-голяма.

70. ЕКЗД и ЕНОЗД считат, че *de facto* общият и неизбирателен автоматизиран анализ на, предавани чрез междуличностни съобщителни услуги, текстови съобщения с цел установяване на потенциални случаи на установяване на контакт с деца не отговаря на изискванията за необходимост и пропорционалност. Дори ако използваната технология е ограничена до прилагането на индикатори, ЕКЗД и ЕНОЗД считат, че въвеждането на такъв общ и неизбирателен анализ е прекомерна мярка и дори може да засегне самата същност на основното право на неприкосновеност на личния живот, залегнало в член 7 от Хартата.

71. Както вече беше посочено, липсата на материалноправни предпазни мерки в контекста на мерките за откриване на случаи на установяване на контакт с деца с цел сексуална злоупотреба не може да бъде компенсирана единствено с процесуални предпазни мерки. Освен това проблемът с липсата на достатъчна правна яснота и сигурност (напр. използването на неясни юридически езикови понятия като „значителна степен“) става още по-сериозен при автоматизирания анализ на текстови лични съобщения, в сравнение със сравняването на снимки въз основа на технология за хеширане.

72. Също така ЕКЗД и ЕНОЗД считат, че „възпиращият ефект“ върху свободата на изразяване на мнение е особено значим, когато текстовите (или звукови) съобщенията на физическите лица се сканират за проверка и анализират повсеместно. ЕКЗД и ЕНОЗД припомнят, че този възпиращ ефект става по-засилен, когато яснотата на закона е намалена.

73. Освен това, както е посочено в доклада за оценка на въздействието [59] и в проучването на Службата на ЕП за парламентарни изследвания [60], точността на технологиите за откриване на случаи на установяване на контакт с деца с цел сексуална злоупотреба въз основа на текстови съобщения е много по-ниска от точността на технологиите за откриване на известни материали, съдържащи СНД [61]. Техниките за откриване на случаи на установяване на контакт с деца са предвидени да анализират и определят вероятностни оценки за всеки аспект на разговора, поради което ЕКЗД и ЕНОЗД също ги считат за податливи на грешки и уязвими от злоупотреби.

[59] Доклад за оценка на въздействието, приложение 8, стр. 281—283.
[60] стр. 15—18.
[61] Вж. по-горе, т. 40.

4.5.7 Заключение относно необходимостта и пропорционалността на предвидените мерки

74. По отношение на необходимостта и пропорционалността на предвидените мерки за откриване ЕКЗД и ЕНОЗД са особено загрижени във връзка с мерките, предвидени за откриване на неизвестни материали, съдържащи СНД, и установяване на контакт с деца („сприятеляване“ с деца) с цел сексуална злоупотреба, поради степента на тяхната намеса при потенциалното предоставяне на достъп до съдържанието на комуникациите на общо основание, вероятностния им характер и процента на грешки във връзка с тези технологии.

75. Още повече че от съдебната практика на Съда на ЕС може да се направи заключението, че мерки, които позволяват на публичните органи да имат достъп на общо основание до съдържанието на дадени комуникации е по-вероятно да засегнат основното съдържание на правата, гарантирани в членове 7 и 8 от Хартата. Тези съображения са особено относими за мерките за откриване на случаи на установяване на контакт с деца с цел сексуална злоупотреба, предвидени в предложението.

76. Във всеки случай ЕКЗД и ЕНОЗД считат, че създаваната намеса, по-специално от мерките за откриване на случаи на установяване на контакт с деца с цел сексуална злоупотреба, надхвърля строго необходимото и пропорционалното. Поради това тези мерки следва да отпаднат от предложението.

4.6 Задължения за докладване

77. ЕКЗД и ЕНОЗД препоръчват списъкът със специфични изисквания за докладване в член 13 от предложението да бъде допълнен с изискване докладът да включва информация относно конкретната технология, която е осигурила възможност на доставчика да установи съответното съдържание, представляващо злоупотреба, в случай че той е узнал за потенциално сексуално насилие над деца вследствие на предприети мерки в изпълнение на заповед за откриване, издадена в съответствие с член 7 от предложението.

4.7 Задължения за премахване и блокиране

78. Една от предвидените в предложението мерки за намаляване на рисковете от разпространение на материали, съдържащи СНД, е издаването на заповеди за премахване и блокиране, които да задължават доставчиците да премахват или блокират достъпа до, или да блокират онлайн материали, съдържащи сексуално насилие над деца.[62]

79. Въпреки че въздействието на заповедите за премахване върху защитата на данните и неприкосновеността на комуникациите е относително ограничено, като обща забележка ЕКЗД и ЕНОЗД припомнят основния принцип, който трябва да се спазва, че всяка подобна мярка следва да бъде възможно най-целенасочена.

80. Същевременно, ЕКЗД и ЕНОЗД обръщат внимание на факта, че доставчиците на услуги за достъп до интернет имат достъп до точния URL адрес на съдържанието само ако това съдържание е предоставено в ясен текст. Всеки път, когато достъпът до съдържанието е чрез HTTPS, доставчикът на услугата за достъп до интернет няма достъп до точния URL, освен ако не наруши криптирането на комуникациите. Поради това ЕКЗД и ЕНОЗД изразяват

[62] Предложението, членове 14 и 16.

съмнение относно ефективността на мерките за блокиране и считат, че изискването от доставчиците на услуги за достъп до интернет да декриптират онлайн комуникациите с цел блокиране на такива, съдържащи СНД, би било непропорционална мярка.

81. Освен това в по-общ план следва да се отбележи, че блокирането (или забраната) на достъпа до даден цифров елемент е операция, която се извършва на равнището на мрежата и нейното прилагане може да се окаже неефективно в случай на множество (евентуално сходни и неидентични) копия на един и същ елемент. Освен това тази операция може да се окаже непропорционална мярка, ако блокирането засяга други цифрови елементи, които не са незаконни, когато те се съхраняват на същия сървър, който е станал недостъпен чрез мрежови команди (например включване в черен списък на IP адреса или DNS). Освен това не всички мрежови подходи към блокирането са еднакво ефективни и някои лесно могат да бъдат заобиколени дори с притежавани по-основни технически умения.

82. И накрая, в предложения регламент следва да бъдат изяснени правомощията на координиращите органи по отношение на издаването на заповеди за блокиране. Например от настоящата формулировка на член 16, параграф 1 и член 17, параграф 1 не е ясно дали координиращите органи са оправомощени да издават или само да изискват издаването на заповеди за блокиране.[63]

4.8 Подходящи технологии и предпазни мерки

4.8.1 Защита на данните при проектирането и по подразбиране

83. Изискванията в предложението, които се прилагат по отношение на технологиите, които следва да бъдат внедрени с цел откриване на материали, съдържащи СНД и случаи на установяване на контакт с деца с цел сексуална злоупотреба, не изглеждат достатъчно строги. По-специално, ЕКЗД и ЕНОЗД отбелязват, че за разлика от аналогичните разпоредби във временния регламент[64], в предложението не се прави изрично позоваване на принципа на защита на данните при проектирането и по подразбиране и не се предвижда, че технологиите, които се използват за сканиране на текст в съобщения, не трябва да са с възможности да правят изводи за същината на съдържанието на съобщенията. В член 10, параграф 3, буква б) от предложението се предвижда само, че технологиите не трябва да са в състояние да „извличат“ друга информация от съответните съобщения, освен информацията, която е строго необходима за откриването. Това изискване обаче не изглежда достатъчно строго, тъй като може да е възможно да се *откриват модели* за друга информация от същността на съдържанието на съобщението, без от него да се *извлича* информация.

84. Поради това ЕНОЗД и ЕКЗД препоръчват в предложението да се включи съображение, в което се посочва, че принципът на защита на данните на етапа на проектирането и по подразбиране, установен в член 25 от Регламент (ЕС) 2016/679, се прилага по отношение на уредените в член 10

[63] Формулировката на член 16, параграф 1 от предложението е следната: „Координиращият орган по място на стопанска дейност има правомощието да поиска от компетентния съдебен орган на държавата членка, която го е определила, или от независим административен орган на тази държава членка да издаде заповед за блокиране, […]“, а формулировката на член 17, параграф 1 е следната „Координиращият орган по място на стопанска дейност издава посочените в член 16 заповеди за блокиране […]“ (подчертаването е добавено).

[64] Временен регламент, член 3, параграф 1, буква б).

от предложението технологии по силата на правото и следователно не е необходимо да се повтаря в правния текст. Освен това член 10, параграф 3, буква б) следва да бъде изменен, за да се гарантира, че не само не се извлича друга информация, но и не се откриват модели, както това е предвидено понастоящем в член 3, параграф 1, буква б) от временния регламент.

4.8.2 Надеждност на технологиите

85. В предложението се приема, че доставчиците на услуги могат да използват няколко вида технологични решения за изпълнение на заповеди за откриване. По-специално в предложението се приема, че са налице системи с изкуствен интелект, които функционират за целите на откриването на неизвестни материали, съдържащи СНД и случаи на установяване на контакт с деца с цел сексуална злоупотреба,[65] и такива технологии могат да се считат за най-съвременни от някои координиращи органи. Въпреки че ефективността на предложението се крепи върху надеждността на такива технологични решения, има много малко информация относно общото и системно използване на такива техники, което изисква внимателното им разглеждане.

86. Освен това трябва да се отбележи, че въпреки че поради липсата на алтернативи ЕКЗД и ЕНОЗД трябваше да използват в своята оценка на пропорционалността индикаторите за ефективност на технологиите за откриване, посочени в доклада за оценка на въздействието, придружаващ предложението, за тези индикатори е предоставена много малко информация за това как е била направена тяхната оценка и дали те отразяват ефективността на съответните технологии в реални условия. Няма информация за изпитванията или референтните стойности, използвани от доставчиците на технологиите за измерване на тези индикатори за ефективност. Без такава информация не е възможно да се повторят изпитванията или да се оцени валидността на изявленията относно индикаторите за ефективност. В това отношение следва да се отбележи, че макар индикаторите за ефективността да могат да се тълкуват като предпоставящи висока точност на някои от инструментите за откриване (напр. точността на някои инструменти за откриване на сприятеляване с деца с цел сексуална злоупотреба е 88 %),[66] тези индикатори следва да се разглеждат с оглед на предвижданата практическа употреба на инструментите за откриване и сериозността на рисковете за съответните субекти на данни, до които би довела една неправилна оценка за съдържанието на даден материал. Освен това ЕКЗД и ЕНОЗД считат, че при такова високорисково обработване, процент на неуспех от 12 % представлява висок риск за субектите на данни, които са станали обект на фалшиви положителни резултати, дори когато са налице предпазни мерки за предотвратяване на подаването на фалшиви доклади до правоприлагащите органи. Много малко вероятно е доставчиците на услуги да заделят достатъчно ресурси за преразглеждане на такъв процент фалшиви положителни резултати.

87. Както беше посочено по-горе,[67] индикаторите за ефективността следва да предоставят изчерпателна информация за поведението на инструментите за откриване. Налице е достатъчно документална информация, че когато се използват алгоритми с изкуствен интелект за изображения или текст, може да възникне изместване и дискриминиране поради липсата на представителност на определени групи от населението в данните, използвани за обучението на алгоритъма. Тези отклонения следва да бъдат установявани, измервани и намалявани до

[65] Вж. Доклад за оценка на въздействието, стр. 281—282.
[66] Пак там, стр. 283.
[67] Вж. т. 63—64 по-горе.

приемливо равнище, за да могат системите за откриване да бъдат наистина от полза за обществото като цяло.

88. Въпреки че е направено проучване на технологиите, използвани за откриване,[68] ЕКЗД и ЕНОЗД считат, че е необходим допълнителен анализ, за да се направи независима оценка на надеждността на използването на съществуващите инструменти в реални условия. Този анализ следва да се основава на изчерпателни индикатори за ефективността и да дава оценка на въздействието на потенциалните грешки в реални условия върху всички субекти на данни, засегнати от предложението. Тъй като тези технологии са основата, на която се основава предложението, ЕКЗД и ЕНОЗД считат, че този анализ е от първостепенно значение за оценката на адекватността на предложението.

89. ЕКЗД и ЕНОЗД отбелязват също, че в предложението не се определят специфични за технологиите изисквания, независимо дали по отношение на процентите на грешка, използването на класификатори и тяхното валидиране или други ограничения. Така разработването на такива критерии за оценката на пропорционалността на използването на конкретна технология се оставя в ръцете на практиката, което допълнително допринася за липсата на прецизност и яснота.

90. Предвид значението на последиците за субектите на данни в случаи на фалшиви положителни резултати, ЕКЗД и ЕНОЗД считат, че процентът на фалшивите положителни резултати трябва да бъде минимален и че при проектирането на тези системи трябва същевременно да се има предвид, че голямата част от електронните съобщения не съдържат материали, съдържащи СНД и случаи на установяване на контакт с деца с цел сексуална злоупотреба, както и че дори когато този процент е много нисък, той ще доведе до много голям брой фалшиви положителни резултати предвид обема на данните, по отношение на които ще се прилагат мерките за откриване. В по-общ план, ЕКЗД и ЕНОЗД са обезпокоени също от факта, че ефективността на наличните инструменти, посочена в доклада за оценка на въздействието, не произтича от точни и сравними индикатори по отношение на фалшивите положителни и фалшивите отрицателни резултати, и считат, че следва да бъдат използвани сравними и пълноценни индикатори за ефективността на тези технологии, преди те да могат да бъдат считани за налични и ефективни.

4.8.3 Сканиране на звукови комуникации

91. За разлика от временния регламент,[69] предложението не изключва от приложното си поле сканирането на звукови комуникации при откриването на случаи на сприятеляване с деца с цел сексуална злоупотреба.[70] ЕКЗД и ЕНОЗД считат, че сканирането на звукови комуникации е с особено висока степен на намеса, тъй като обикновено налага активно и текущо прихващане „на живо“. Още повече, че в някои държави членки неприкосновеността на говора се ползва със специална закрила.[71] Освен това, поради факта, че по принцип ще трябва да се анализира цялото съдържание на звуковото съобщение, много е вероятно тази мярка да засегне същността на правата, гарантирани в членове 7 и 8 от Хартата. Поради това този метод за откриване следва да остане извън обхвата на задълженията за откриване, определени в предложения регламент,

[68] Вж. Доклад за оценка на въздействието, стр. 279 и сл.
[69] Вж. временния регламент, член 1, параграф 2.
[70] Вж. предложението, член 1.
[71] Вж. напр. германския наказателен кодекс, раздел 201.

както по отношение на гласовите съобщения, така и по отношение на комуникация „на живо“, още повече с оглед на факта, че в доклада за оценка на въздействието, който придружава предложението, не са установени никакви конкретни рискове или промени в аспектите на заплахите, които биха обосновали използването му.[72]

4.8.4 Проверка на възрастта

92. Предложението насърчава доставчиците да използват мерки за проверка и определяне на възрастта, за да установяват децата — ползватели на техните услуги.[73] По отношение на това ЕКЗД и ЕНОЗД отбелязват, че понастоящем не съществува технологично решение, което да е способно да определи със сигурност възрастта на даден ползвател в онлайн контекст без да се разчита на официална цифрова самоличност, която на този етап не е достъпна за всеки европейски гражданин.[74] Поради това предвиденото в предложението прилагане на мерки за проверка на възрастта би могло да доведе до изключване от достъп до онлайн услуги напр. на лица, които изглеждат млади, или до внедряването на инструменти за проверка на възрастта с висока степен на намеса, което може да възпрепятства или да обезкуражи използването със законна цел на въпросните услуги.

93. В това отношение и въпреки че съображение 16 от предложението се позовава на инструменти за родителски контрол като възможни мерки за намаляване на риска, ЕКЗД и ЕНОЗД препоръчват предложеният регламент да бъде изменен, за да се даде изрично възможност на доставчиците да се основават на механизми за родителски контрол в допълнение или като алтернатива на проверката на възрастта.

4.9 Съхраняване на информацията

94. Член 22 от предложението ограничава целите, за които доставчиците, предмет на предложението, могат да запазват данните за съдържанието и другите данни, обработвани във връзка с мерките, предприети за спазване на определените им в предложението задължения. В предложението обаче се посочва, че доставчиците могат също така да запазят тази информация с цел подобряване на ефективността и точността на технологиите за откриване на онлайн сексуално насилие над деца за изпълнение на заповед за откриване, но те не могат да съхраняват никакви лични данни за тази цел.[75]

95. ЕКЗД и ЕНОЗД считат, че само тези доставчици, които използват собствени технологии за откриване следва да имат право да запазват данни с цел подобряване на ефективността и точността на технологиите, докато тези, които използват технологии, предоставени от Центъра на ЕС, не следва да се ползват от тази възможност. Освен това, ЕКЗД и ЕНОЗД отбелязват, че на практика може да е трудно да се гарантира, че няма да се съхраняват лични данни с такава цел, тъй като повечето данни за съдържанието и другите данни, обработвани за целите на откриването, е най-вероятно да се квалифицират като лични данни.

---

[72] Вж. доклада за оценка на въздействието.

[73] Вж. предложението, член 4, параграф 3, член 6, параграф 1, буква в) и съображение 16.

[74] Вж. напр. CNIL, Препоръка 7: Проверка на възрастта на дете със съгласието на родителите при зачитане на личната неприкосновеност на детето (9 август 2021 г.).

[75] Предложението, член 22, параграф 1.

4.10 Въздействие върху криптирането

96. Европейските органи в областта на защита на данните последователно се застъпват за широкото разпространение на силни инструменти за криптиране и се противопоставят на всякакъв вид задни вратички.[76] Това е така, защото криптирането е важно, за да се гарантира упражняването на всички права на човека офлайн и онлайн.[77] Освен това технологиите за криптиране допринасят съществено както за зачитането на личния живот и поверителността на комуникациите, така и за иновациите и растежа на цифровата икономика, която разчита на високото равнище на доверие и сигурност, които тези технологии осигуряват.

97. По отношение на междуличностните съобщения криптирането „от край до край“ („E2EE“) е ключов инструмент за гарантиране на поверителността на електронните съобщения, тъй като осигурява силни технически предпазни мерки срещу достъпа до съдържанието на съобщенията от всеки друг освен изпращача и получателя (получателите), включително срещу достъпа от доставчика. Непозволяването или възпирането по какъвто и да е начин на използването на E2EE, налагането на задължение на доставчиците на услуги да обработват данни от електронни съобщения за цели, различни от предоставянето на техните услуги, или налагането на задължение за проактивно препращане на електронни съобщения към трети страни, би довело до риск доставчиците да предлагат по-слабо криптирани услуги с цел по-добро спазване на задълженията, като по този начин би се отслабила ролята на криптирането като цяло и би се подкопало зачитането на основните права на европейските граждани. Следва да се отбележи, че въпреки че E2EE е една от най-често използваните мерки за сигурност при електронните съобщения, също толкова важни за сигурността и защитата на поверителността на цифровите комуникации могат да бъдат или да станат и други технически решения (напр. използването на други криптографски схеми). Поради това тяхното използване също не следва да бъде предотвратявано или възпирано.

98. Внедряването на инструменти за прихващане и анализ на междуличностни електронни съобщения по същество противоречи на E2EE, тъй като последното има за цел технически да гарантира, че комуникацията между изпращача и получателя запазва поверителния си характер.

99. Поради това, въпреки че в предложението не се определя задължение за доставчиците да извършват системно прихващане, самата възможност за издаване на заповед за откриване вероятно ще окаже сериозно влияние върху избора на технически средства, който ще направят доставчиците, особено като се има предвид ограниченият срок, който ще имат, за да изпълнят такава заповед и тежките санкции, които биха им били наложени, ако не го направят.[78] На практика това може да накара някои доставчици да спрат да използват E2EE.

100. Въздействието на влошаването на E2EE или възпирането от прилагането му, което може да се получи в резултат на предложението, трябва да бъде оценено по подходящ начин. Всяка от техниките за заобикаляне на поверителния характер на E2EE, представени в доклада за оценка

[76] Вж. напр. становището на Работната група по член 29 за защита на личните данни относно криптирането и въздействието върху защитата на физическите лица във връзка с обработването на техните лични данни в ЕС (11 април 2018 г.).
[77] Вж. Резолюция 47/16 на Съвета по правата на човека относно утвърждаването, защитата и упражняването на правата на човека в интернет, документ на ООНА/HRC/RES/47/16 (26 юли 2021 г.).
[78] Вж. предложението, член 35.

на въздействието, който придружава предложението, ще доведе до пропуски в сигурността.[79] Например сканирането откъм клиента[80] вероятно ще доведе до значителен, нецеленасочен достъп до устройствата на крайния потребител и обработване на некриптирано съдържание в тях. Такова значително влошаване на поверителността ще засегне особено децата, тъй като е по-вероятно услугите, които те използват, да станат предмет на заповеди за откриване, което ги прави уязвими от наблюдение или подслушване. В същото време сканирането откъм сървърите също е напълно несъвместимо с парадигмата на E2EE, тъй като ще е необходимо да бъде нарушен криптираният „от точка до точка" комуникационен канал, което ще доведе до масово обработване на лични данни на сървърите на доставчиците.

101. Въпреки че в предложението се посочва, че то „предоставя на съответния доставчик избора на технологиите, които да използва, за да изпълни ефикасно заповедите за откриване, и това не следва да се разбира като насърчаване или разубеждаване да се използва дадена технология, ...", [81] структурната несъвместимост на дадена заповед за откриване с E2EE на практика се превръща в силен демотивиращ фактор за използването на E2EE. Невъзможността за достъп и ползване на услуги с прилагане на E2EE (които представляват съвременното технологично равнище по отношение на техническото гарантиране на поверителността) може да има възпиращ ефект върху свободата на изразяване на мнение и законното използване за лични цели на електронни съобщителни услуги. Неблагоприятната връзка между E2EE и откриването на материали, съдържащи СНД и случаи на установяване на контакт с деца с цел сексуална злоупотреба, се признава също така и от Комисията, която в доклада си за оценка на въздействието[82] отбелязва вероятността прилагането на E2EE от Facebook през 2023 г. да доведе до прекратяване на сканирането по собствена инициатива от Facebook.

102. За да се гарантира, че предложеният регламент не накърнява сигурността или поверителността на електронните комуникации на европейските граждани, ЕКЗД и ЕНОЗД считат, че в постановителната част на предложението следва ясно да се посочва, че нищо в предложения регламент не следва да се тълкува като забрана или отслабване на криптирането, в съответствие с посоченото в съображение 25 от временния регламент.

4.11 Надзор, правоприлагане и сътрудничество

4.11.1 Функции на националните надзорни органи съгласно ОРЗД

103. Предложението предвижда създаването на мрежа от национални координиращи органи, които отговарят за изпълнението на предложения регламент и правоприлагането.[83] Въпреки че в съображение 54 от предложението се посочва, че „Правилата на настоящия регламент относно надзора и правоприлагането не следва да се разбират като засягащи правомощията и

[79] Вж. раздел 4.2 в Abelson, Harold, Ross J. Anderson, Steven M. Bellovin, Josh Benaloh, Matt Blaze, John L Callas, Whitfield Diffie, Susan Landau, Peter G. Neumann, Ronald L. Rivest, Jeffrey I. Schiller, Bruce Schneier, Vanessa Teague и Carmela Troncoso, „Техническите дефекти в нашия джоб: Рисковете на сканирането от страна на клиента", arXiv abs/2110.07450 (2021).

[80] Сканирането от страна на клиента най-общо се отнася до системи, които сканират съдържанието на съобщенията за съвпадения с база данни с неотговарящо на изискванията съдържание, преди съобщението да бъде изпратено на предвидения получател.

[81] Предложението, съображение 26.

[82] Доклад за оценка на въздействието, стр. 27.

[83] Предложението, член 25.

компетентността на органите за защита на данните съгласно Регламент (ЕС) 2016/679“, ЕКЗД и ЕНОЗД са на мнение, че следва да бъде по-добре регламентирана връзката между задачите на координиращите органи и тези на органите за защита на данните и че на органите за защита на данните следва да бъде отредена по-важна роля в рамките на предложения регламент.

104. По-специално от доставчиците следва да се изисква да се консултират с органите за защита на данните в рамките на процедура за предварителна консултация, както това е посочено в член 36 от ОРЗД, преди въвеждането на мерки за откриване на сексуална злоупотреба с деца или сприятеляване с деца с цел сексуална злоупотреба, а не само във връзка с използването на мерки за откриване на случаи на сприятеляване с деца с цел сексуална злоупотреба, както е предвидено понастоящем в предложението.[84] Всички мерки за откриване следва да се считат за водещи до „висок риск“ по подразбиране и поради това за тях следва да бъде проведена процедура на предварителна консултация, независимо от това дали се отнасят до сприятеляване с деца с цел сексуална злоупотреба или до материали, съдържащи СНД, което вече е регламентирано във временния регламент.[85] Освен това компетентните органи за защита на данните, определени съгласно ОРЗД, следва да имат правомощието във всички случаи да предоставят своите становища относно предвидените мерки за откриване, а не само при конкретни обстоятелства.[86]

105. Освен това с предложения регламент следва да се създаде система за разглеждане и намиране на решения на разногласия между компетентните органи и органите за защита на данните по отношение на заповедите за откриване. По-специално, на органите за защита на данните следва да се предостави правото да оспорват заповед за откриване пред съдилищата на държавата членка на компетентния съдебен орган или независимия административен орган, издал заповедта. В тази връзка ЕКЗД и ЕНОЗД отбелязват, че съгласно настоящата версия на предложението становището на компетентните органи за защита на данните може да бъде отхвърлено от компетентния орган при издаването на заповед за откриване. Това може потенциално да доведе до противоречащи си решения, тъй като както се потвърждава от разпоредбите на член 36, параграф 2 от ОРЗД, органите за защита на данните запазват пълния набор от корективните си правомощия съгласно член 58 от ОРЗД, включително правомощието да разпоредят забрана на обработването.

4.11.2 Функции на ЕКЗД

106. ЕКЗД и ЕНОЗД отбелязват, че в член 50, параграф 1, трето изречение от предложението се предвижда, че „... Центърът на ЕС изисква становището на своя Комитет по технологии и на Европейския комитет по защита на данните.“, преди да включи конкретна технология към списъците с технологии, които доставчиците на хостинг услуги и доставчиците на междуличностни съобщителни услуги могат да използват, за да изпълняват заповеди за откриване. Освен това в него се предвижда, че ЕКЗД представя становищата си в срок от осем седмици, които при необходимост могат да бъдат удължени с още шест седмици, като се вземе предвид сложността на въпроса. И накрая, в предложението се изисква ЕКЗД да уведомява

[84] Предложението, член 7, параграф 3, второ тире, буква б).
[85] Временен регламент, член 3, параграф 1), буква в).
[86] Вж. предложението, член 7, параграф 3, второ тире, буква в).

Центъра на ЕС в срок до един месец от получаване на искането за консултация за всяко такова удължаване, включително и за причините за забавянето.

107. Съществуващите задачи на ЕКЗД са определени в член 70 от ОРЗД и член 51 от Директива (ЕС) 2016/680 (по-нататък „ДПЗД“).[87] В тези задачи се посочва, че ЕКЗД консултира Комисията и предоставя становища по искане на Комисията, на национален надзорен орган или на неговия председател. Въпреки че в член 1, параграф 3, буква г) от предложението се посочва, че предложението не засяга правилата, установени в ОРЗД и в ДПЗД, оправомощаването на Центъра на ЕС да изисква становища от ЕКЗД надхвърля обхвата на задачите, възложени на ЕКЗД съгласно ОРЗД и ДПЗД. Поради това в предложения регламент — поне в съображение — следва да се поясни, че предложението разширява задачите на ЕКЗД. Във връзка с това ЕКЗД и ЕНОЗД ценят важната роля, която се отрежда на ЕКЗД в предложението, и изискването за участието му в практическото прилагане на предложения регламент. На практика секретариатът на ЕКЗД има съществена роля за предоставянето на необходимата аналитична, административна и логистична подкрепа за приемането на становища от ЕКЗД. Поради това, за да се гарантира, че ЕКЗД и неговите членове ще могат да изпълняват своите задачи, от съществено значение е да се определи достатъчен бюджет и персонал за ЕКЗД. За съжаление обаче в законодателната финансова обосновка на предложението не се посочва, че ще бъдат предоставени допълнителни ресурси за изпълнението на допълнителните задачи, които се възлагат на ЕКЗД в предложението.[88]

108. Освен това ЕКЗД и ЕНОЗД отбелязват, че в член 50 от предложението не се посочва как ще процедира Центърът на ЕС след получаване на становище от ЕКЗД.[89] В съображение 27 от предложението се посочва само, че съветите, предоставени от ЕКЗД, следва да се вземат предвид от Центъра на ЕС и Европейската комисия. Поради това следва да се изясни каква е целта на исканото становище в процеса, предвиден в член 50 от предложението, и какви действия следва да предприеме Центърът на ЕС след като получи становище от ЕКЗД.

109. Също така ЕКЗД и ЕНОЗД считат, че въпреки че всички дадени насоки или евентуално становище на ЕКЗД относно използването на технологии за откриване ще съдържат оценка на приложението на такива технологии на общо основание, за предварителната консултация съгласно член 36 от ОРЗД е необходимо националният надзорен орган да вземе предвид конкретните обстоятелства и да извърши оценка за всеки отделен случай на планирано обработване от съответния администратор. ЕКЗД и ЕНОЗД отбелязват, че надзорните органи прилагат и следва да прилагат критериите, посочени в член 36 от ОРЗД, когато решават дали е необходимо да се удължи определеният в ОРЗД срок за предоставяне на становищата им в отговор на процедура по предварителна консултация, и не е необходимо да се прилагат различни стандарти, когато предварителната консултация се отнася до използването на технология за откриване.[90]

---

[87] Директива (ЕС) 2016/680 на Европейския парламент и на Съвета от 27 април 2016 г. относно защитата на физическите лица във връзка с обработването на лични данни от компетентните органи за целите на предотвратяването, разследването, разкриването или наказателното преследване на престъпления или изпълнението на наказания и относно свободното движение на такива данни, и за отмяна на Рамково решение 2008/977/ПВР на Съвета (ОВ L 119, 4.5.2016 г., стр. 89—131).

[88] Вж. предложението, стр. 105 и сл.

[89] Вж. за разлика от това член 51, параграф 4 от ДПЗД.

[90] Вж. Предложението, съображение 24.

110. И накрая, при прилагането на член 11 („Насоки относно задълженията за откриване“) от предложението е предвидено, че Комисията може да издава насоки относно прилагането на членове 7—10 от предложението. Член 11 от предложението следва да бъде изменен, за да се поясни, че освен с координиращите органи и Центъра на ЕС, Комисията следва да се консултира и с ЕКЗД относно проекта за насоки, извън предвидения процес на обществена консултация, преди да издаде насоки относно задълженията за откриване.

111. Поради това тази задача на ЕКЗД, както и функцията му в правната рамка, която ще бъде въведена с предложението, налага допълнителна оценка от страна на законодателя.

4.11.3 Функции на Центъра на ЕС за предотвратяване и противодействие на сексуалното насилие над деца

112. С глава IV от предложението се предвижда да се създаде Центърът на ЕС като нова децентрализирана агенция, която ще осигури възможност за изпълнение на предложението. Наред с другите си задачи, Центърът на ЕС следва да улеснява достъпа на доставчиците до надеждни технологии за откриване; предоставя индикатори, създадени въз основа на онлайн сексуално насилие над деца и проверени от съдилища или независими административни органи на държавите членки за целите на откриването; и предоставя подкрепа при комуникацията със съответните национални органи.[91]

113. Във връзка с това ЕКЗД и ЕНОЗД приветстват член 77, параграф 1 от предложението, в който се потвърждава, че обработването на лични данни от Центъра на ЕС се извършва съгласно РЗДЕС, и се предвижда, че мерките за прилагането на посочения регламент от Центъра на ЕС, включително тези относно назначаването на длъжностно лице по защита на данните в Центъра на ЕС, се определят след консултация с ЕНОЗД. ЕКЗД и ЕНОЗД обаче са на мнение, че няколко разпоредби от тази глава трябва да бъдат разгледани по-задълбочено.

114. На първо място, ЕКЗД и ЕНОЗД отбелязват, че в член 48 от предложението се предвижда всички доклади, които не са „явно неоснователни“[92], да се препращат на националните правоприлагащи органи и на Агенцията на ЕС за сътрудничество в областта на правоприлагането („Европол“). Това прагово условие за препращане на докладите от Центъра на ЕС на националните правоприлагащи органи и Европол (когато са „явно неоснователни“) изглежда твърде занижено, особено като се има предвид, че целта на създаването на Центъра на ЕС, както това е посочено в доклада на Комисията за оценка на въздействието,[93] е да се облекчи тежестта за правоприлагащите органи и Европол от филтрирането на съдържание, погрешно обозначено като материали, съдържащи СНД. В това отношение не е ясно защо Центърът на ЕС, в качеството му на експертен център, не би могъл да извършва по-задълбочен правен и фактически анализ с цел да се ограничат рисковете от предаване на данни на невинни лица на правоприлагащите органи.

115. На второ място разпоредбата относно продължителността на съхранение на лични данни от Центъра на ЕС изглежда относително отворена предвид чувствителния характер на съответните данни. Дори и да не е възможно да се определи максимален срок за съхранение на тези данни,

---

[91] Вж. COM(2022) 209 final, стр. 7.

[92] Понятието „явно неоснователни“ е разгледано в съображение 65 от предложението като „когато е очевидно, без да е необходим задълбочен правен или фактически анализ, че докладваните дейности не представляват онлайн сексуално насилие над деца.“

[93] Вж. например стр. 349 от доклада за оценка на въздействието.

ЕКЗД и ЕНОЗД препоръчват в предложението да се определи най-малкото максимален срок, след който да се преразгледа необходимостта от продължаване на съхранението на данните и да се изисква обосноваване при удължаване на срока на съхранение след този срок.

116. Освен това, предвид много високата чувствителност на личните данни, които ще се обработват от Центъра на ЕС, ЕКЗД и ЕНОЗД са на мнение, че за обработването следва да се прилагат допълнителни предпазни мерки, по-специално, за да се гарантира ефективен надзор. Това би могло да включва задължението на Центъра на ЕС да поддържа записи за операциите по обработване на данни в системите за автоматизирано обработване (т.е. огледално изискване на това за лични данни от оперативен характер съгласно глава IX от РЗДЕС), включително регистриране на въвеждането, промяната, достъпа, извършването на справка, разкриването, комбинирането и заличаването на лични данни. Записите за извършена справка или разкриване следва да дават възможност за установяване на основанието за това, както и датата, и часа на такива операции, самоличността на лицето, което е направило справка или е разкрило лични данни от оперативен характер, и — доколкото е възможно, самоличността на получателите. Тези записи могат да се използват за проверка на законосъобразността на обработването, за гарантиране на неговия интегритет и сигурност и за самонаблюдение, и ще се предоставят при поискване на длъжностното лице по защита на данните в Центъра на ЕС и на ЕНОЗД.

117. Освен това в предложението се посочва задължението на доставчиците да информират потребителите, когато открият материали, съдържащи СНД чрез заповеди за откриване, както и за правото им да подават жалби до координиращия орган.[94] В предложението обаче не се определя редът, по който субектите на данни упражняват правата си, предвид също така множеството места, където личните данни могат да бъдат предавани и съхранявани съгласно предложението (Центъра на ЕС, Европол, националните правоприлагащи агенции). В изискването за информиране на потребителите следва да се включи задължението за информиране на физическите лица, когато техните данни са препратени и се обработват от други органи, когато случаят е такъв (напр. от националните правоприлагащи органи и Европол). Освен това следва да има централизирана процедура за получаване и координиране на искания за право на достъп, коригиране и заличаване или, като друга възможност, задължение органът, който получи искане от субект на данни, да координира действията си с другите засегнати органи.

118. ЕКЗД и ЕНОЗД отбелязват, че съгласно член 50 от предложението Центърът на ЕС има за задача да състави списък на технологиите, които могат да се използват за изпълнението на заповеди за откриване. Съгласно член 12, параграф 1 от предложението обаче доставчиците са задължени да докладват всяка информация, показваща потенциално онлайн сексуално насилие над деца в техните услуги, а не само информацията, произтичаща от изпълнението на заповед за откриване. Много вероятно е значителна част от тази информация да дойде от прилагането на мерки за намаляване на риска от доставчиците в съответствие с член 4 от предложението. Следователно е от решаващо значение да се определи какви биха могли да бъдат тези мерки, тяхната ефективност, процентът на грешки при докладването на потенциални случаи на сексуално насилие над деца и какво е тяхното въздействие върху правата и свободите на лицата. Въпреки факта, че в член 4, параграф 5 от предложението се посочва, че в сътрудничество с координиращите органи и Центъра на ЕС и след провеждане на обществена консултация, Комисията може да издаде съответните насоки, ЕКЗД и ЕНОЗД считат, че е важно законодателят

[94] Вж. член 10, параграф 6 и, след представянето на доклад до Центъра на ЕС, член 12, параграф 2 от предложението.

да включи в член 50а задача на Центъра на ЕС да предостави също така списък с препоръчителни мерки за намаляване на риска и съответни най-добри практики, които са особено ефективни при установяването на потенциално онлайн сексуално насилие над деца. Тъй като такива мерки могат да представляват намеса в основните права на защита на данните и неприкосновеност на личния живот, препоръчително е също така Центърът на ЕС да изиска становището на ЕКЗД, преди да оповести такъв списък.

119. И накрая, изискванията за сигурност, посочени в член 51, параграф 4 от предложението, следва да бъдат по-конкретни. В това отношение може да се почерпи опит от изискванията за сигурност, установени в други регламенти по отношение на широкомащабните системи, в които се осъществява високорисково обработване, като Регламент 767/2008 [95] (вж. член 32), Регламент 1987/2006 [96] (вж. член 16), Регламент 2018/1862 [97] (вж. член 16) и Регламент 603/2013[98] (вж. член 34).

4.11.4 Функции на Европол

120. Предложението предвижда тясно сътрудничество между Центъра на ЕС и Европол. Съгласно глава IV от предложението, при получаване на доклади от доставчици относно предполагаеми материали, съдържащи СНД, Центърът на ЕС ги проверява, за да прецени кои доклади подлежат на разглеждане (не са явно неоснователни) и ги препраща на Европол, както и на националните правоприлагащи органи.[99] Центърът на ЕС предоставя на Европол достъп до своите бази данни с индикатори и бази данни с доклади с цел оказване на съдействие за разследванията от Европол на предполагаеми престъпления, свързани със сексуално насилие над деца.[100] Освен това на Центъра на ЕС ще бъде предоставен „възможно най-пълен“ достъп до

[95] Регламент (ЕО) № 767/2008 на Европейския парламент и на Съвета от 9 юли 2008 г. относно Визовата информационна система (ВИС) и обмена на данни между държави членки относно визите за краткосрочно пребиваване (Регламент за ВИС), ОВ L 218, 13.8.2008 г., стр. 60–81.

[96] Регламент (ЕО) № 1987/2006 на Европейския парламент и на Съвета от 20 декември 2006 г. за създаването, функционирането и използването на Шенгенска информационна система от второ поколение (ШИС II), (ОВ L 381, 28.12.2006 г., стр. 4—23).

[97] Регламент (ЕС) 2018/1862 на Европейския парламент и на Съвета от 28 ноември 2018 г. за създаването, функционирането и използването на Шенгенската информационна система (ШИС) в областта на полицейското сътрудничество и съдебното сътрудничество по наказателноправни въпроси, за изменение и отмяна на Решение 2007/533/ПВР на Съвета и за отмяна на Регламент (ЕО) № 1986/2006 на Европейския парламент и на Съвета и Решение 2010/261/ЕС на Комисията (ОВ L 312, 7.12.2018 г., стр. 56—106).

[98] Регламент (ЕС) № 603/2013 на Европейския парламент и на Съвета от 26 юни 2013 г. за създаване на система Евродак за сравняване на дактилоскопични отпечатъци с оглед ефективното прилагане на Регламент (ЕС) № 604/2013 за установяване на критерии и механизми за определяне на държавата членка, компетентна за разглеждането на молба за международна закрила, която е подадена в една от държавите членки от гражданин на трета държава или от лице без гражданство, и за искане на сравнения с данни в Евродак от правоприлагащите органи на държавите членки и Европол за целите на правоприлагането и за изменение на Регламент (ЕС) № 1077/2011 за създаване на Европейска агенция за оперативното управление на широкомащабни информационни системи в пространството на свобода, сигурност и правосъдие (ОВ L 180, 29.6.2013 г., стр. 1—30).

[99] Вж. член 48 от предложението.

[100] Вж. член 46, параграфи 4—5 от предложението.

информационните системи на Европол.[101] Двете агенции също така ще споделят помещения и определена (неоперативна) инфраструктура.[102]

121. ЕКЗД и ЕНОЗД отбелязват, че няколко аспекта, свързани със сътрудничеството между предложения Център на ЕС и Европол пораждат загриженост или е необходимо да бъдат допълнително уточнени.

Относно изпращането на доклади от Центъра на ЕС на Европол (член 48)

122. В член 48 от предложения регламент се изисква Центърът на ЕС да препраща доклади, за които прецени, че не са явно неоснователни, заедно с всякаква допълнителна относима информация, на Европол и на компетентния правоприлагащ орган или органи на държавата членка, който е вероятно да е компетентен/които е вероятно да са компетентни да разследват или да повдигнат обвинение за потенциалното сексуално насилие над деца. Въпреки че с този член се възлага на Европол функция да определя съответния правоприлагащ орган при неясна ситуация относно съответната държава членка, с разпоредбата всъщност се предвижда, че всички доклади се предават на Европол, без значение дали националният орган е установен и докладът е предаден към него от Центъра на ЕС.

123. В предложението обаче не се изяснява каква би била добавената стойност от участието на Европол или очакваната му функция при получаването на докладите, особено в случаите, когато националният правоприлагащ орган е установен и уведомен успоредно с това.[103]

124. ЕКЗД и ЕНОЗД припомнят, че мандатът на Европол е ограничен до оказването на подкрепа за действията на компетентните органи на държавите членки и взаимното им сътрудничество за предотвратяване и борба с тежката престъпност, засягаща две или повече държави членки.[104] В член 19 от Регламент (ЕС) 2016/794[105], изменен с Регламент (ЕС) 2022/991[106] („изменения Регламент за Европол“), се предвижда, че орган на Съюза, който предоставя информация на Европол, определя целта или целите, с оглед на която(ито) се обработва информация от Европол, както и условията за обработването. Агенцията отговаря също за гарантиране на точността на предавани лични данни.[107]

---

[101] Вж. член 53, параграф 2 от предложението.

[102] По-специално тези, свързани с управлението на човешките ресурси, информационните технологии (ИТ), включително киберсигурността, сгради и комуникации.

[103] В съображение 71 от предложението се прави само общо позоваване на опита на Европол при установяването на компетентните национални органи в неясна ситуация и предвид нейната база данни със сведения за целите на наказателни разследвания, която може да допринесе за откриване на връзки с разследвания в други държави членки.

[104] Вж. член 3 от изменения регламент за Европол.

[105] 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—114).

[106] Регламент (ЕС) 2022/991 на Европейския парламент и на Съвета от 8 юни 2022 г. за изменение на Регламент (ЕС) 2016/794 по отношение на сътрудничеството на Европол с частноправни субекти, обработването на лични данни от Европол в подкрепа на наказателни разследвания и ролята на Европол в областта на научните изследвания и иновациите (ОВ L 169, 27.6.2022 г., стр. 1—42).

[107] Член 38, параграф 2, буква а) от изменения регламент за Европол.

125. Следователно препращането на общо основание на доклади към Европол би било в противоречие с изменения регламент за Европол и може да носи редица рискове за защитата на данните. Дублирането на обработването на лични данни би могло да доведе до паралелно съхраняване на множество копия на едни и същи изключително чувствителни лични данни (например в Центъра на ЕС, Европол, националния правоприлагащ орган), с рискове за точността на данните в резултат на потенциалното десинхронизиране на базите данни, както и за упражняването на правата на субектите на данни. Освен това установените в предложението ниски прагови изисквания за споделяне на докладите с правоприлагащите органи (такива, които „не са явно неоснователни“) предполагат висока вероятност в информационните системи на Европол да бъдат съхранявани потенциално за продължителни периоди от време фалшиви положителни резултати (т.е. съдържание, погрешно обозначено като материали, съдържащи сексуално насилие над деца).[108]

126. Поради това ЕКЗД и ЕНОЗД препоръчват в предложението да се определят и ограничат обстоятелствата и целите, при които Центърът на ЕС би могъл да препраща доклади на Европол, в съответствие с изменения регламент за Европол. Това следва изрично да изключва обстоятелствата, при които докладите се предават на правоприлагащия орган на съответната държава членка, което предполага, че не е налице трансгранично измерение. Освен това в предложението следва да бъде включено изискването Центърът на ЕС да предава на Европол само лични данни, които са подходящи, относими и ограничени до строго необходимото. Трябва да се предвидят също и специфични предпазни мерки за гарантиране на качеството и надеждността на данните.

Член 53, параграф 2 относно сътрудничеството между Центъра на ЕС и Европол

127. В член 53, параграф 2 от предложението се определя изискване Европол и Центърът на ЕС да си предоставят взаимно „възможно най-пълен достъп до относимата информация и до съответните информационни системи, когато това е необходимо за изпълнението на съответните им задачи и в съответствие с актовете на правото на Съюза, уреждащи този достъп“.

128. В член 46, параграфи 4 и 5 от предложението допълнително се уточнява, че Европол има достъп до базата данни на Центъра на ЕС с индикатори и базата данни с доклади, а в член 46, параграф 6 се определя процедурата за предоставяне на този достъп: Европол подава искане, в което се посочват целта на искането и степента на достъп, необходима за постигането на тази цел, и искането се оценява старателно от Центъра на ЕС.

129. Критериите и предпазните мерки, които обуславят достъпа на Европол и последващото използване на данни, получени от информационните системи на Центъра на ЕС, не са уточнени. Освен това не е пояснено защо е необходимо да се предоставя на Европол пряк достъп до информационните системи, на агенция с област на дейност извън правоприлагането, които съдържат силно чувствителни лични данни, чиято връзка с престъпна дейност и предотвратяването на престъпността може да не е установена. С цел да се гарантира високо

[108] Според доклада на Комисията за оценка на въздействието Европол е бил в състояние да разгледа едва 20 % от 50-те милиона уникални изображения и видеоматериали, съдържащи СНД, в своята база данни, което предполага липса на ресурси за разглеждане на постъпили материалите, съдържащи СНД, които агенцията текущо получава. Вж. доклада за оценка на въздействието, придружаващ предложението за регламент за определяне на правила за предотвратяване и борба със сексуалното насилие над деца, SWD (2022) 209, стр. 47—48.

равнище на защита на данните и спазване на принципа на ограничаване в рамките на целта, ЕКЗД и ЕНОЗД препоръчват предаването на лични данни от Центъра на ЕС към Европол да се извършва само според отделните индивидуални случаи, след старателна оценка на искането и посредством инструмент за сигурен комуникационен обмен, като например SIENA.[109]

130. В член 53, параграф 2 е предложено единственото позоваване на актовете на правото на Съюза във връзка с достъпа на Центъра на ЕС до информационните системи на Европол. Следователно не е ясно за какви цели и при какви конкретни гаранции ще се осъществява такъв достъп.

131. ЕКЗД и ЕНОЗД припомнят, че Европол е агенция в областта на правоприлагането, създадена съгласно Договорите на ЕС с основен мандат за предотвратяване и борба с тежката престъпност. Следователно по отношение на личните данни от оперативен характер, обработвани от Европол, се прилагат строги правила и предпазни мерки. Предложеният център на ЕС не е правоприлагащ орган и при никакви обстоятелства не следва да му се предоставя пряк достъп до информационните системи на Европол.

132. ЕКЗД и ЕНОЗД отбелязват също така, че голяма част от информацията от общ интерес за Центъра на ЕС и Европол ще се отнася до лични данни, свързани с жертви на предполагаеми престъпления, лични данни на непълнолетни и малолетни лица и лични данни относно сексуалния живот, които се определят като специални категории лични данни съгласно изменения регламент за Европол. Измененият регламент за Европол налага строги условия по отношение на достъпа до специалните категории лични данни. В член 30, параграф 3 от изменения Регламент за Европол се посочва, че само Европол има пряк достъп до такива лични данни, и по-специално само ограничен брой длъжностни лица на Европол, надлежно упълномощени от изпълнителния директор.[110]

133. Поради това ЕКЗД и ЕНОЗД препоръчват да се поясни формулировката на член 53, параграф 2 от предложението с цел тя да отразява правилно ограниченията, въведени съгласно изменения регламент за Европол, и да се уточнят условията за достъп на Центъра на ЕС. По-специално, всеки достъп до лични данни, обработвани в информационните системи на Европол, когато се счита за строго необходим за изпълнението на задачите на Центъра на ЕС, следва да се предоставя само според отделния случай и след подадено изрично искане, в което е документирана конкретната цел и основанието за обработването. От Европол следва да се изисква да извършва старателна оценка на тези искания и да предава лични данни на Центъра на ЕС само когато това е строго необходимо и пропорционално на изискваната цел.

Член 10, параграф 6 относно функцията на Европол за информиране на ползвателите след изпълнението на заповед за откриване

134. ЕКЗД и ЕНОЗД приветстват изискването, посочено в член 10, параграф 6 от предложението, доставчиците да информират ползвателите, чиито лични данни могат да бъдат засегнати от изпълнението на заповед за откриване. Тази информация се предоставя на ползвателите само след получаване на потвърждение от Европол или от националния правоприлагащ орган на държава членка, получила доклада съгласно член 48 от предложението, че информирането на

[109] Приложение за мрежа за сигурен обмен на информация (SIENA).

[110] Съгласно изменения Регламент за Европол изключения от тази забрана са предвидени за агенциите на Съюза, създадени съгласно дял V от ДФЕС. Като се има предвид обаче правното основание за предложението (чл. 114 от ДФЕС във връзка с хармонизирането на вътрешния пазар), това изключение не би включвало предложения Център на ЕС.

ползвателите няма да попречи на дейностите за предотвратяване, откриване, разследване и наказателно преследване на престъпления, свързани със сексуално насилие над деца.

135. Липсва обаче конкретност по отношение на прилагането на практика на тази разпоредба. Когато докладите се препращат едновременно на Европол и на правоприлагащ орган на държава членка, в предложението не се посочва дали е необходимо потвърждение от единия или от двамата получатели, нито са посочени процедурите/редът и условията за получаване на такова потвърждение (например дали потвържденията се изпращат чрез Центъра на ЕС). Като се има предвид големият обем материали, съдържащи СНД, които Европол и националните правоприлагащи органи може да се налага да обработват, както и липсата на точен срок за предоставяне на потвърждение („без ненужно забавяне“), ЕКЗД и ЕНОЗД препоръчват да се изяснят приложимите процедури, за да се гарантира действието на тази предпазна мярка на практика. Освен това към задължението за информиране на ползвателите следва да се включва и информация относно получателите на съответните лични данни.

Относно събирането на данни и докладването за прозрачност (член 83)

136. В член 83, параграф 3 от предложението се предвижда Центърът на ЕС да събира данни и да генерира статистически данни, свързани с редица от неговите задачи съгласно предложения регламент. За целите на мониторинга ЕКЗД и ЕНОЗД препоръчват в този списък да се добавят статистически данни относно броя на докладите, препратени на Европол в съответствие с член 48, както и броя на исканията за достъп, получени от Европол съгласно член 46, параграфи 4 и 5, включително броя на исканията, които са одобрени и са получили отказ от Центъра на ЕС.

5. ЗАКЛЮЧЕНИЕ

137. Въпреки че ЕКЗД и ЕНОЗД приветстват усилията на Комисията да гарантира ефективни действия срещу онлайн сексуалното насилие над деца, те считат, че предложението поражда сериозни опасения относно защитата на данните и неприкосновеността на личния живот. Поради това ЕКЗД и ЕНОЗД приканват съзаконодателите да изменят предложения регламент, по-специално за да се гарантира, че предвидените задължения за откриване отговарят на приложимите изисквания за необходимост и пропорционалност и не водят до отслабване или влошаване качеството на криптирането на общо основание. ЕКЗД и ЕНОЗД остават на разположение, за да окажат подкрепа по време на законодателния процес, ако тяхното участие в него бъде счетено за необходимо за намиране на решения на опасенията, очертани в настоящото съвместно становище.

За Европейския надзорен орган по защита на данните

Европейски надзорен орган по защита на данните

(Wojciech Wiewiorowski)

За Европейския комитет по защита на данните

Председател

(Andrea Jelinek)