Насоки № 2/2023 относно техническия обхват на член 5, параграф 3 от Директивата за правото на неприкосновеност на личния живот и електронни комуникации

Версия 2.0

Приети на 7 октомври 2024 г.

История на версиите

Версия 1.0	14 ноември 2023 г.	Приемане на насоките за обществена консултация
Версия 2.0	7 октомври 2024 г.	Приемане на насоките след обществена консултация

Кратко изложение

В настоящите насоки ЕНОЗД разглежда приложимостта на член 5, параграф 3 от Директивата за правото на неприкосновеност на личния живот и електронни комуникации към различни технически решения. Настоящите насоки разширяват обхвата на Становище 9/2014 на Работната група по член 29 относно прилагането на Директивата за правото на неприкосновеност на личния живот и електронни комуникации към отпечатъците на устройства и имат за цел да осигурят ясно разбиране на техническите операции, обхванати от член 5, параграф 3 от Директивата за правото на неприкосновеност на личния живот и електронни комуникации.

Появата на нови методи за проследяване, които заместват съществуващите инструменти (например „бисквитки“ поради прекратената поддръжка на „бисквитки“ на трети страни от някои доставчици на браузъри) и създават нови бизнес модели, се превърна в критично важен проблем за защитата на данните. Въпреки че приложимостта на член 5, параграф 3 от Директивата за правото на неприкосновеност на личния живот и електронни комуникации е добре установена и се прилага за някои технологии за проследяване, например „бисквитките“, е необходимо да се отстранят неяснотите, свързани с прилагането на посочената разпоредба към новите инструменти за проследяване.

В Насоките се посочват три ключови елемента за приложимостта на член 5, параграф 3 от Директивата за правото на неприкосновеност на личния живот и електронни комуникации (раздел 2.1), а именно „информация“, „крайно оборудване на абонат или потребител“ и „получаване на достъп“ и „съхранение на информация и съхранена информация“. Освен това насоките предоставят подробен анализ на всеки елемент (раздел 2.2—2.6).

В раздел 3 този анализ е приложен към неизчерпателен списък от случаи на употреба, представляващи общи техники, а именно:

- URL и проследяване на пиксели
- Локална обработка
- Проследяване само въз основа на IP
- Периодично и опосредствано отчитане на интернет на нещата (IoT)
- Уникален идентификатор

Съдържание

Европейският комитет по защита на данните,

като взе предвид член 70, параграф 1, буква д) от 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 и за отмяна на Директива 95/46/ЕО (наричан по-нататък „ОРЗД“),

като взе предвид Споразумението за Европейското икономическо пространство, и по-специално приложение XI и протокол 37 към него, изменено с Решение на Съвместния комитет на ЕИП № 154/2018 от 6 юли 2018 г.[1],

като взе предвид член 15, параграф 3 от Директива 2002/58/ЕО на Европейския парламент и на Съвета от 12 юли 2002 г. относно обработката на лични данни и защита на правото на неприкосновеност на личния живот в сектора на електронните комуникации, изменена с Директива 2009/136/ЕО (наричана по-нататък „Директивата за правото на неприкосновеност на личния живот и електронни комуникации“ или „ДПНЕК“),

като взе предвид членове 12 и 22 от своя Правилник за дейността,

ПРИЕ СЛЕДНИТЕ НАСОКИ:

1 ВЪВЕДЕНИЕ

1. Съгласно член 5, параграф 3 *от ДПНЕК „съхраняването на информация или получаването на достъп до информация, вече съхранявана в крайното оборудване на абоната или ползвателя,“* е позволено само въз основа на съгласие или необходимост за конкретни цели, посочени в същия член. Както се напомня в съображение 24 от ДПНЕК[2], целта на тази разпоредба е да се защитят крайното оборудване на потребителите, тъй като те са част от частната сфера на потребителите. От формулировката на члена следва, че член 5, параграф 3 от Директивата за електронните услуги не се прилага единствено за „бисквитките“, а и за „подобни технологии“. Понастоящем обаче не съществува изчерпателен списък на техническите операции, обхванати от член 5, параграф 3 от Директивата.

2. В становище 9/2014 на Работната група по член 29 (наричана по-нататък „РГ 29“) относно прилагането на Директивата за правото на неприкосновеност на личния живот и електронни комуникации по отношение на отпечатъците на устройства (наричано по-нататък „Становище 9/2014 на Работната група по член 29“) вече беше пояснено, че отпечатъците попадат в

[1] Позоваванията на „държави членки“ в настоящия документ следва да се разбират като позовавания на „държави — членки на ЕИП“.

[2] Крайното оборудване на потребителите на електронни комуникационни мрежи и всяка информация, съхранявана в такова оборудване, се отнасят до частния живот на потребителите, изискващ защита съгласно Европейската конвенция за защита на човешките права и основните свободи. Т.нар. шпионски софтуер, пикселни маркери, скрити идентификатори и други подобни устройства могат да проникнат в крайното устройство на потребителя без негово знание, за да получат достъп до информация, да съхраняват скрита информация или да проследяват дейностите на потребителя и могат сериозно да нарушат неприкосновеността на личния живот на тези потребители. Използването на такива устройства следва да бъде разрешено само за законни цели, със знанието на съответните потребители.

техническия обхват на член 5, параграф 3 от ДПНЕК[3], но поради новия напредък в технологиите са необходими допълнителни насоки по отношение на наблюдаваните понастоящем техники на проследяване. Техническата обстановка претърпя развитие през последното десетилетие с нарастващото използване на идентификатори, вградени в операционните системи, както и със създаването на нови инструменти, позволяващи съхранението на информация в крайните устройства.

3. Неяснотите по отношение на приложното поле на член 5, параграф 3 от ДПНЕК създават стимули за прилагане на алтернативни решения за проследяване на потребителите на интернет и водят до тенденция за заобикаляне на правните задължения, предвидени в този член. Всички такива ситуации пораждат загриженост и изискват допълнителен анализ, с оглед допълване на предишните насоки на ЕКЗД.

4. Целта на настоящите насоки е да се извърши технически анализ на обхвата на прилагане на член 5, параграф 3 от ДПНЕК, а именно да се изяснят техническите аспекти, обхванати от фразата *„за съхраняване на информация или за получаване на достъп до информация, съхранявана в крайното оборудване на абонат или потребител“*. В настоящия документ не се разглеждат обстоятелствата, при които дадена операция по обработване може да попадне в обхвата на изключенията от изискването за съгласие, предвидени в Директивата[4], тъй като тези обстоятелства следва да се анализират за всеки отделен случай, като се отчитат транспонирането(ята) в съответната(ите) държава(и) членка(и) и насоките, издадени от националните компетентни органи.

5. Неизчерпателен списък на конкретни случаи на използване ще бъде анализиран в заключителната част на настоящите насоки.

2 АНАЛИЗ

2.1 Основни елементи за приложимостта на член 5, параграф 3 от ДПНЕК

6. Член 5, параграф 3 от ДПНЕК се прилага, ако:

   a. **КРИТЕРИЙ А:** извършените операции се отнасят до *„информация“*. Следва да се отбележи, че използваният термин не е „лични данни“, а „информация“.

   b. **КРИТЕРИЙ Б:** извършените операции включват *„крайно оборудване“* на абонат или потребител (Б.1), което предполага необходимостта от оценка на понятието *за „обществена съобщителна мрежа“* (Б.2).

   c. **КРИТЕРИЙ В** извършените операции действително представляват *„съхранение“* (В.1) или *„получаване на достъп“* (В.2). Тези две понятия могат да бъдат проучени независимо, както се припомня в Становище 9/2014 на Работната група по член 29: *„Използването на думите „която се съхранява или до която се получава достъп показва“, че не е необходимо*

[3] Становище 9/2014 на РГ 29, стр. 11.

[4] Както е посочено в член 5, параграф 3 от ДПНЕК: *„Това не пречи на всякакво техническо съхранение или достъп с единствена цел осъществяване на предаването на съобщение по електронна съобщителна мрежа или доколкото е строго необходимо, за да може доставчикът да предостави услуга на информационното общество, изрично поискана от абоната или ползвателя.“*

съхранението и достъпът да се осъществяват в рамките на една и съща комуникация и не е необходимо да се извършват от една и съща страна.“[5]

За улеснение на четенето субектът, който получава достъп до информацията, съхранявана в крайното оборудване на потребителя, ще бъде наричан по-долу „субект, който извършва достъп“.

2.2 Понятието „информация“ — критерий А

7. Както е посочено в КРИТЕРИЙ А, в този раздел се описва подробно какво се включва в понятието „информация“. Изборът на термина „информация“, който обхваща по-широка категория от самото понятие за лични данни, е свързан с обхвата на Директивата за правото на неприкосновеност на личния живот и електронни комуникации.

8. Целта на член 5, параграф 3 от Директивата за електронните услуги е да се защити личната сфера на потребителите, както е посочено в съображение 24 от нея: *„Крайното оборудване на потребителите на електронни комуникационни мрежи и всяка информация, съхранявана в такова оборудване, се отнасят до частния живот на потребителите, изискващ защита съгласно Европейската конвенция за защита на човешките права и основните свободи.“* То е защитено и от член 7 от Хартата на основните права на ЕС.

9. Всъщност сценариите, които навлизат в тази частна сфера, дори без да включват лични данни, са изрично обхванати от текста на член 5, параграф 3 и съображение 24 от ДПНЕК, например съхраняването на вируси в крайното оборудване на потребителя. Това показва, че определението на понятието „информация“ не следва да се ограничава до свойството да бъде свързана с идентифицирано физическо лице или физическо лице, което може да бъде идентифицирано.

10. Това е потвърдено от Съда на ЕС: *„Тази защита се прилага за всяка информация, съхранявана в такова крайно оборудване, независимо дали става дума за лични данни, и както следва от същото съображение, има по-специално за цел да защити потребителите срещу риска скрити идентификатори и други подобни устройства да проникнат в крайното им оборудване без тяхно знание.“*[6].

11. Въпросите за това дали произходът на тази информация и причините, поради които тя се съхранява в крайното оборудване, следва да се вземат предвид при оценката на приложимостта на член 5, параграф 3 от ДПНЕК, бяха изяснени по-рано. Например в Становище 9/2014 на РГ 29: *„Не е правилно това да се тълкува в смисъл, че третата страна не изисква съгласие за достъп до тази информация, просто защото не я е съхранявала. Изискването за съгласие се прилага и когато се осъществява достъп до стойност, предназначена само за четене (напр. искане на MAC адрес на мрежов интерфейс чрез API на операционната система).“* [7]

12. В заключение, понятието „информация“ включва както нелични, така и лични данни, независимо от начина, по който тези данни са били съхранявани и от кого, т.е. дали от външен субект (включително и други субекти, различни от този, който има достъп), от ползвателя, от производителя или по друг начин.

[5] Становище 9/2014 на РГ 29, стр. 8.
[6] Решение на Съда от 1 октомври 2019 г., Planet 49, дело C-673/17, ECLI:EU:C:2019:801, точка 70.
[7] Становище 9/2014 на РГ 29, стр. 8.

2.3 Понятието „крайно оборудване на абонат или потребител“ — критерий Б.1

13. Настоящият раздел се основава на определението, използвано в Директива 2008/63/ЕО и както е посочено в член 2 от Директива (ЕС) 2018/1972, където „крайно оборудване“ се определя като: *„устройство, предназначено за пряко или непряко свързване към интерфейс на обществена далекосъобщителна мрежа за пренасяне, обработка и приемане на информация; и в двата случая, пряко или непряко, свързването може да бъде осъществено чрез жици, оптични влакна или електромагнитен път; свързването е непряко, ако устройството е поставено между крайното устройство и интерфейса на обществената мрежа“* [8].

14. Съображение 24 от ДПНЕК дава ясна представа за ролята на крайното оборудване за защитата, предлагана от член 5, параграф 3 от ДПНЕК. Директивата защитава неприкосновеността на личния живот на потребителите не само по отношение на поверителността на тяхната информация, но и чрез запазване на целостта на крайното оборудване на потребителя. Това разбиране ръководи тълкуването на понятието „крайно оборудване“ в настоящите насоки.

15. В член 3 се посочва, че за да се прилага Директивата, обработването на лични данни трябва да се извършва във връзка с предоставянето на обществено достъпни електронни съобщителни услуги в обществени съобщителни мрежи. Това означава, че едно устройство трябва да може да се използва във връзка с такава услуга и че, за да бъде определено като крайно оборудване, то трябва да бъде свързано или да може да се свърже[9] с интерфейса на обществена съобщителна мрежа. ЕКЗД отбелязва, че измененията, направени през 2009 г.[10] в текста на член 5, параграф 3 от ДПНЕК, разширяват защитата на крайното оборудване, като заличават позоваването на „използването на електронна съобщителна мрежа“ като средство за съхраняване на информация или за получаване на достъп до информация, съхранявана в крайното оборудване. Следователно, докато дадено устройство има мрежов интерфейс, който го прави годно за свързване (дори и да не е налице такова свързване), член 5, параграф 3 от ДПНЕК се прилага за всеки субект, който съхранява и получава достъп до информация, която вече се съхранява в крайното оборудване, независимо от начина на достъп до крайното оборудване и независимо от това дали то е свързано или не с мрежа.

16. Оборудване, което е част от самата обществена електронна съобщителна мрежа, няма да се счита за крайно оборудване съгласно член 5, параграф 3 от ДПНЕК[11].

17. Крайното оборудване може да се състои от какъвто и да е брой отделни части от хардуера, които заедно образуват крайното оборудване. Това може да бъде или не под формата на физически затворено устройство, в което е разположен целия хардуер, включващ екрани, процесори,

---

Директива 2008/63/ЕО на Комисията от 20 юни 2008 г. относно конкуренцията на пазарите на крайни далекосъобщителни устройства (кодифицирана версия), член 1, параграф 1.

[9] Това означава да има технически възможности за свързване с мрежата, дори ако тази връзка понастоящем не е налице.

[10] Директива 2009/136/ЕО на Европейския парламент и на Съвета от 25 ноември 2009 г. за изменение на Директива 2002/22/ЕО относно универсалната услуга и правата на потребителите във връзка с електронните съобщителни мрежи и услуги, Директива 2002/58/ЕО относно обработката на лични данни и защита на правото на неприкосновеност на личния живот в сектора на електронните комуникации и Регламент (ЕО) № 2006/2004 за сътрудничество между националните органи, отговорни за прилагане на законодателството за защита на потребителите (Текст от значение за ЕИП), ОВ L 337, 18.12.2009 г., член 2, параграф 5 и съображение 65.

[11] За определяне на границите на мрежата в различен контекст, направете справка с Насоките на ОЕРЕС относно общите подходи за определяне на точката за приключване на мрежата в различни мрежови топологии (BoR (20) 46).

устройства за съхранение и периферни устройства (напр. смартфони, лаптопи, мрежови устройства за съхранение, свързани автомобили или свързани телевизори, интелигентни очила).

18. Директивата отчита, че защитата на поверителността на информацията, съхранявана в крайното оборудване на потребителя, както и целостта на оборудването не се ограничава до защитата на личната сфера на физическите лица, а засяга и правото на зачитане на тяхната кореспонденция или законните интереси на юридическите лица[12]. По този начин крайното оборудване, което позволява осъществяването на тази кореспонденция и законните интереси на юридическите лица, е защитено съгласно член 5, параграф 3 от ДПНЕК.

19. Потребителят или абонатът може да бъде притежател или наемател на крайното оборудване, или то да му бъде предоставено по друг начин. Множество потребители или абонати могат да споделят едно и също крайно оборудване.

20. Тази защита е гарантирана от ДПНЕК за крайното оборудване, свързано с потребителя или абоната, и не зависи от това дали потребителят е създал средствата за достъп (например ако е инициирал електронната комуникация) или дори от това дали потребителят знае за посочените средства за достъп.)

2.4 Понятие за „обществена съобщителна мрежа“ — критерий Б.2

21. Тъй като случаите, регламентирани в ДПНЕК, са свързани с *„предоставянето на обществено достъпна електронна съобщителна услуга в Общността“* [13], а в определението за крайно оборудване изрично се споменава понятието *„обществена съобщителна мрежа“*, от решаващо значение е да се изясни това понятие, за да се определи контекстът, в който се прилага член 5, параграф 3 от Директивата за електронната неприкосновеност.

22. Понятието „електронна съобщителна мрежа“ не е определено в самата ДПНЕК. Това понятие първоначално е посочено в Директива 2002/21/ЕО (Рамкова директива) относно общата регулаторна рамка за електронните съобщителни мрежи и услуги[14], впоследствие заменено с член 2, параграф 1 от Директива (ЕС) 2018/1972 (Европейски кодекс за електронни съобщения). Понастоящем текстът гласи:

> *„електронна съобщителна мрежа“ означава преносни системи, независимо дали са базирани на постоянна инфраструктура, или на централизиран административен капацитет, и когато е приложимо, оборудване за комутация или маршрутизация и други ресурси, включително неактивни мрежови елементи, които позволяват преноса на сигнали посредством проводници, радиовълни, оптични или други електромагнитни способи, включително спътникови мрежи, фиксирани (с комутация на канали и пакети, включително интернет) и мобилни мрежи, електропроводни системи, доколкото са използвани за пренос на сигнали, мрежи, използвани за радио- и телевизионно*

[12] Всъщност, както се припомня в член 2 (13) от Директива (ЕС) 2018/1972 на Европейския парламент и на Съвета от 11 декември 2018 г. за установяване на Европейски кодекс за електронни съобщения, потребителят може да бъде физическо или юридическо лице.
[13] Член 3 от ДПНЕК.
[14] Директива 2002/21/ЕО на Европейския парламент и на Съвета от 7 март 2002 година относно общата регулаторна рамка за електронните съобщителни мрежи и услуги (Рамкова директива)

разпръскване, кабелни телевизионни мрежи, независимо от типа на пренасяната информация;[15]

23. Това определение е неутрално по отношение на технологиите за предаване. Съгласно него, електронна съобщителна мрежа е всяка мрежова система, която позволява предаване на електронни сигнали между нейните възли, независимо от използваното оборудване и протоколи.

24. Понятието за електронна съобщителна мрежа съгласно Директива 2018/1972 не зависи от публичния или частния характер на инфраструктурата, нито от начина, по който мрежата се внедрява или управлява (*„независимо дали е базирана на постоянна инфраструктура, или на централизиран административен капацитет“*[16]. В резултат на това, определението за електронна съобщителна мрежа съгласно член 2 от Директива 2018/1972 е достатъчно широко, за да обхваща всякакъв вид инфраструктура. То включва мрежи, управлявани или не от оператор, мрежи, управлявани съвместно от група оператори, или дори *ad-hoc* мрежи, в които крайно оборудване може динамично да бъде свързвано или изключвано от друго крайно оборудване, използвайки протоколи за предаване на данни на къси разстояния.

25. Това определение за мрежа не поставя никакво ограничение по отношение на броя на крайните устройства, намиращи се в мрежата по всяко време. Някои схеми за създаване на мрежи разчитат на възли, които предават информация *ad hoc* на възли, които понастоящем са свързани[17], и в даден момент могат да имат поне две свързани равноправни устройства. Такива случаи биха били в рамките на общия обхват на Директивата, при условие че мрежовият протокол позволява по-нататъшно включване на равноправни устройства.

26. Публичната достъпност на комуникационната мрежа е необходима, за да може устройството да се счита за крайно оборудване и следователно, за да се прилага член 5, параграф 3 от ДПНЕК. Следва да се отбележи, че фактът, че мрежата се предоставя на ограничена част от обществеността (например абонати, независимо дали плащат или не, при спазване на условията за допустимост), не прави такава мрежа частна[18].

2.5 Понятие за „получаване на достъп“ — критерий В.1

27. За да се формулира правилно понятието „получаване на достъп“, е важно да се разгледа обхватът на ДПНЕК, посочен в член 1 от нея: *„осигуряване на еднаква степен на защита на основните права и свободи, и по-специално правото на неприкосновеност на личния живот и правото на поверителност по отношение на обработката на лични данни в електронно съобщителния сектор и да се осигури свободно движение на такива данни и оборудване за електронни съобщения и услуги в Общността.“*

[15] Директива (ЕС) 2018/1972 на Европейския парламент и на Съвета от 11 декември 2018 г. за установяване на Европейски кодекс за електронни съобщения (преработена), текст от значение за ЕИП, член 2, параграф 1

[16] Директива (ЕС) 2018/1972 на Европейския парламент и на Съвета от 11 декември 2018 г. за установяване на Европейски кодекс за електронни съобщения (преработена), текст от значение за ЕИП, член 2, параграф 1

[17] Например в контекста на мрежови схеми, устойчиви на забавяне, които прилагат техники за съхраняване и препращане, като проекта с отворен код Briar.

[18] За допълнителен анализ на идентифицирането на обществените съобщителни мрежи вж. Насоките на ОЕРЕС относно прилагането на Регламента за отворен интернет (BoR (20) 112).

28. Накратко, Директивата е правен инструмент за запазване на неприкосновеността на личния живот, който има за цел да защити поверителността на съобщенията и целостта на устройствата. В съображение 24 от ДПНЕК е пояснено, че когато става въпрос за физически лица, крайното устройство на ползвателя е част от тяхната частна сфера и че достъпът до информация, съхранявана в нея без тяхното знание, може сериозно да наруши неприкосновеността на личния им живот.

29. Юридическите лица също са защитени от ДПНЕК[19]. Следователно понятието „получаване на достъп“ по член 5, параграф 3 от Директивата трябва да се тълкува по начин, който защитава тези права срещу нарушение от страна на трети лица.

30. Съхраняването на информация или получаването на достъп могат да бъдат независими операции и да се извършват от независими субекти. Не е необходимо да са налице едновременно съхраняване на информация и достъп до вече съхранена информация, за да се приложи член 5, параграф 3 от ДПНЕК.

31. Както е посочено в Становище 9/2014 на Работната група по член 29: *„Използването на думите „която се съхранява или до която се получава достъп показва“, че не е необходимо съхранението и достъпът да се осъществяват в рамките на една и съща комуникация и не е необходимо да се извършват от една и съща страна. Поради това информацията, която се съхранява от една от страните (включително информация, съхранявана от потребителя или производителя на устройството), до която друга страна по-късно осъществява достъп, попада в обхвата на член 5, параграф 3*“[20]. Следователно няма ограничения за произхода на информацията в крайното оборудване, за да се приложи понятието за достъп.

32. Когато даден субект предприема стъпки за получаване на достъп до информацията, съхранявана в крайното оборудване, се прилага член 5, параграф 3 от ДПНЕК. Обикновено това означава, че субектът, който извършва достъп, трябва проактивно да изпраща конкретни инструкции на крайното оборудване, за да получи обратно целевата информация. Такъв е например случаят с „бисквитките“, където субект, който извършва достъп, инструктира крайното оборудване да изпраща проактивно информация при всяка следваща заявка чрез протокола за пренос на хипертекст (HTTP).

33. Това важи и за случаите, когато субект, който извършва достъп, разпределя на крайното оборудване на потребителя софтуер, който се съхранява и след това активно извиква по мрежата крайна точка на приложно-програмен интерфейс (API). Допълнителните примери включват код в JavaScript, с който субект, извършващ достъп, инструктира браузъра на потребителя да изпраща асинхронни искания с целевата информация. Такъв достъп очевидно попада в обхвата на член 5, параграф 3 от Директивата, тъй като субект, който извършва достъп, изрично инструктира крайното оборудване да изпрати информацията.

34. В някои случаи субектът, който дава инструкции на крайното оборудване да изпрати обратно целевите данни, и субектът, който получава информацията, може да не е един и същ. Това може да се дължи на предоставянето и/или използването на общ механизъм между двата субекта. Инструктирането на устройството да изпраща вече съхранена информация (например чрез използването на протокол или на SDK,[21] което предполага проактивно изпращане на

[19] Съображение 26 от ДПНЕК, вж. точка 17 по-горе.

[20] Становище 9/2014 на РГ 29, стр. 8.

[21] SDK („комплект за разработване на софтуер“) е пакет от инструменти за разработване на софтуер, които се предоставят за улесняване на създаването на приложен софтуер.

информация от крайното устройство) прави възможно проникване в крайното оборудване, поради което такъв достъп задейства член 5, параграф 3. Както е отбелязано в Становище 09/2014 на Работната група по член 29, това може да се случи, когато даден уебсайт инструктира крайното оборудване да изпраща информация до рекламни услуги на трети страни чрез включването на проследяващ пиксел[22]. Този случай на употреба е допълнително разгледан в раздел 3.1.

2.6 Понятията „съхранение на информация“ и „съхранена информация“ — критерий B.2

35. Съхранението на информация по смисъла на член 5, параграф 3 от ДПНЕК се отнася до записването на информация на физически електронен носител, който е част от крайното оборудване на потребителя или абоната[23].

36. Обикновено информацията не се съхранява в крайното оборудване на потребителя или абоната чрез пряк достъп на друго лице до паметта на устройството, а по-скоро чрез даване на указания на софтуера на крайното устройство да генерира конкретна информация. Съхранението, което се извършва чрез такива указания, се счита за започнато пряко от другата страна. Това включва използването на установени протоколи, например съхранение на бисквитки в браузъра, както и персонализиран софтуер, независимо от това кой е създал или инсталирал протоколите или софтуера на крайното оборудване.

37. В Директивата не се поставя горна или долна граница за продължителността на времето, през което информацията трябва да се съхранява на носител на информация, за да се счита за съхранена, нито горна или долна граница за обема на информацията, която трябва да се съхранява.

38. По същия начин понятието за съхранение не зависи от вида на носителя, на който се запазва информацията. Типичните примери включват твърди дискове („HDD“), полупроводникови дискови устройства („SSD“), електрически изтриваема програмируема памет само за четене (EEPROM) и памет с произволен достъп (RAM), но не са изключени от обхвата на приложение по-малко типични сценарии, включващи среда като магнитна лента или кеш памет на централен процесор (CPU). Запаметяващото устройство може да бъде свързано вътрешно (напр. чрез SATA връзка) или външно (напр. чрез USB връзка).

39. „Съхранявана информация“ се отнася до информация, която вече съществува на крайното устройство, независимо от източника или естеството на тази информация. Това включва всеки резултат от съхранението на информация по смисъла на член 5, параграф 3 от ДПНЕК, както е описано по-горе (или от същата страна, която по-късно ще получи достъп, или от друга трета страна). Освен това включва резултати от процеси за съхранение на информация извън обхвата на член 5, параграф 3 от ДПНЕК, например: съхранение на крайното оборудване от самия потребител или абонат или от производител на хардуер (напр. MAC адреси на контролери на мрежови интерфейси), датчици, интегрирани в крайното оборудване, или процеси и програми, изпълнявани върху крайното оборудване, които могат или не могат да генерират информация, която зависи от съхраняваната информация или е извлечена от нея.

[22] Становище 9/2014 на РГ 29, стр. 9.

[23] Както е определено в точка 2.3 от настоящите насоки.

3 СЛУЧАИ НА УПОТРЕБА

40. Както е посочено във въведението към настоящите насоки[24], в тях не се анализира прилагането на изключенията от задължението за получаване на съгласие, предвидено в член 5, параграф 3 от ДПНЕК. ЕКЗД напомня, че във всички случаи, когато има съхраняване на информация или получаване на достъп до вече съхранявана информация, ще трябва да се прецени дали е необходимо съгласие или дали може да се прилага изключение по член 5, параграф 3, буква д) от Директивата. Поради това читателят следва да разгледа изключенията в техния случай на употреба във връзка с този технически анализ.

41. Без да се засяга специфичният контекст, в който могат да се използват тези технически категории, които са необходими, за да се определи дали е приложим член 5, параграф 3 от ДПНЕК, е възможно да се определят по неизчерпателен начин широки категории идентификатори и информация, които са широко използвани и могат да бъдат обхванати от член 5, параграф 3 от ДПНЕК.

42. Комуникацията в мрежата обикновено се основава на многостепенен модел, който изисква използването на идентификатори, за да се даде възможност за правилно установяване и осъществяване на комуникацията. Предаването на тези идентификатори на дистанционните участници се извършва чрез софтуер съгласно договорените протоколи за комуникация. Както е посочено по-горе, фактът, че получаващият субект може да не е субектът, който дава инструкции за изпращане на информация, не изключва прилагането на член 5, параграф 3 от ДПНЕК. Това може да се отнася до маршрутни идентификатори като MAC или IP адреса на крайното оборудване, но също така и идентификатори на сесиите (SSRC, идентификатор на Websocket) или токени за удостоверяване на автентичността.

43. По същия начин протоколът на приложението може да включва няколко механизма за предоставяне на данни за контекста (например HTTP заглавие, включващо поле „accept“ (приемане), или потребителски агент), механизъм за кеширане (например ETag[25]) или други функционалности (бисквитките са една от тях или HSTS[26]). Отново, разчитането на тези механизми за събиране на информация (например във връзка със снемането на пръстови отпечатъци[27] или проследяването на идентификаторите на ресурси) може да доведе до прилагането на член 5, параграф 3 от ДПНЕК.

44. От друга страна, налице са случаи, при които локалните приложения, инсталирани в крайното оборудване, използват определена информация строго вътре в терминала, какъвто може да е случаят с API на системата за смартфони (достъп до камера, микрофон, GPS сензор, чип за ускорител, радиочип, локален достъп до файлове, списък с контакти, достъп до идентификатори и др.). Такъв може да бъде случаят и с уеб браузърите, които обработват съхранявана или генерирана информация в рамките на устройството (например бисквитки, местно съхранение, WebSQL или дори информация, предоставена от самите потребители). Използването на такава информация от дадено приложение няма да представлява „получаване на достъп до вече

[24] Вж. точка 4 по-горе.

[25] HTTP ETag е идентификатор, който позволява да се направи условно искане въз основа на валидността на кешираните данни на клиента.

[26] Http Strict Transport Security (HSTS) позволява на сървърите да уточнят кои ресурси следва винаги да се изискват, като се използват връзки с HTTPS.

[27] Както е отбелязано във въведението, вижте Становище 9/2014 на Работната група по член 29 относно прилагането на Директивата за правото на неприкосновеност на личния живот и електронни комуникации към отпечатъците на устройствата.

съхранена информация“ по смисъла на член 5, параграф 3 от ДПНЕК, докато информацията не напуска устройството, но когато се получи достъп до тази информация или до всяко нейно производно, ще се приложи гореспоменатата разпоредба от Директивата.

45. И накрая, в някои случаи участниците разпространяват зловреден софтуер, например софтуер за добив на криптовалути или по-общо казано зловреден софтуер, като използват възможностите за обработка на данни на крайното оборудване в полза на разпространяващия участник. Разпространението на посочения злонамерен софтуер в крайното оборудване на потребителя представлява „съхранение“ по смисъла на член 5, параграф 3 от ДПНЕК. Освен това, ако софтуерът установи мрежова връзка, за да изпрати информация на по-късен етап, това представлявало „получаване на достъп“ по смисъла на член 5, параграф 3 от ДПНЕК.

46. По-долу е представен специфичен анализ за подгрупата от тези категории, които представляват особен интерес, било поради широкото им използване, било поради това, че е оправдано провеждането на специално проучване по отношение на обстоятелствата, при които те се използват.

3.1 URL и проследяване на пиксели

47. Проследяващият пиксел е хипервръзка към ресурс, обикновено файл с изображение, вграден в част от съдържание като уебсайт или имейл. Този пиксел обикновено не изпълнява никаква цел, свързана със самото заявено съдържание; единствената му цел е автоматично да установи комуникация от страна на клиента към хоста на пиксела, която иначе не би се осъществила. Това обаче не е систематично и пикселите за проследяване могат да бъдат създадени и чрез добавяне на допълнителна информация към изображенията за зареждане на хипервръзки, които са свързани със съдържанието, показвано на потребителя. Установяването на комуникацията предава различна информация на хоста на пиксела в зависимост от конкретния случай на използване.

48. В случай на електронно писмо изпращачът може да включи проследяващ пиксел, за да открие кога получателят ще прочете електронното съобщение. Последяващите пиксели в уебсайтовете могат да се свържат с организация, която събира много такива заявки и по този начин може да проследява поведението на потребителите. Тези проследяващи пиксели могат също така да съдържат допълнителни идентификатори, метаданни или съдържание като част от връзката. Тези данни могат да бъдат добавени от собственика на уебсайта, евентуално свързани с дейността на потребителя на този уебсайт, така че да могат да се генерират аналитични отчети за използването му. Те могат също така да бъдат динамично генерирани чрез приложна логика от страната на клиента, предоставена от субекта.

49. Връзките за проследяване могат да функционират по същия начин, но идентификаторът се добавя към адреса на уебсайта. Когато потребителят посещава единния ресурсен локатор (URL), целевият уебсайт зарежда искания ресурс, но също така събира идентификатор, който не е от значение по отношение на идентификацията на ресурсите. Те много често се използват от уебсайтове за електронна търговия за идентифициране на произхода на техния входящ източник на трафик. Например такива уебсайтове могат да предоставят на партньорите си проследявани връзки, които да използват в техния домейн, така че уебсайтът за електронна търговия да знае кой от партньорите му е отговорен за продажбата и да плати комисиона — практика, известна като партньорски маркетинг.

50. Както връзките за проследяване, така и пикселите за проследяване могат да се разпределят по най-различни канали, например чрез имейли, уебсайтове или дори, в случай на връзки за

проследяване — чрез всякакви системи за текстови съобщения. Това разпространение до крайното оборудване на потребителя представлява съхранение, най-малкото чрез механизма за кеширане на софтуера от страна на клиента. В този смисъл член 5, параграф 3 от ДПНЕК е приложим, дори ако това съхранение не е постоянно.

51. Добавянето на информация за проследяване към URL адреси или изображения (пиксели), изпратени на потребителя, представлява инструкция към крайното устройство да изпрати обратно целевата информация (определения идентификатор). В случай на динамично конструирани проследяващи пиксели инструкцията се изразява в разпределение на приложната логика (обикновено код в JavaScript). Вследствие на това може да се счита, че събирането на идентификатори, предоставени чрез такива механизми за проследяване, представлява „получаване на достъп“ по смисъла на член 5, параграф 3 от ДПНЕК, поради което се прилага и за тази стъпка.

3.2 Локална обработка

52. Някои технологии разчитат на локална обработка, наредена от софтуер, разпределен в крайното оборудване на потребителите, където след това информацията, генерирана от локалната обработка, се предоставя на избрани участници чрез приложно-програмен интерфейс (API) от страна на клиента. Такъв може да бъде например случаят с API, предоставен от уеб браузъра, където локално генерираните резултати могат да бъдат достъпни от разстояние.

53. Ако в който и да е момент, например в кода на клиента, обработената информация се предоставя на трета страна, например изпратена обратно по мрежата на сървър, такава операция (наредена от субекта, създаващ кода на клиента в потребителското крайно устройство) би представлявала „получаване на достъп до информация, която вече се съхранява“. Фактът, че тази информация се произвежда локално, не изключва прилагането на член 5, параграф 3 от Директивата.

3.3 Проследяване само въз основа на IP

54. Някои доставчици разработват решения, които разчитат само на събирането на един компонент, а именно IP адреса, за да проследят навигацията[28] на потребителя, в някои случаи в няколко домейна. В този смисъл член 5, параграф 3 от ДПНЕК би могъл да се приложи, въпреки че инструкцията за предоставяне на IP адрес е дадена от субект, различен от получателя.

55. Получаването на достъп до IP адреси обаче води до прилагането на член 5, параграф 3 от ДПНЕК само в случаите, когато тази информация произхожда от крайното оборудване на абоната или потребителя. Въпреки че това не е систематично (например когато[29] се задейства CGNAT), статичният изходящ IPv4 с произход от рутера на потребителя попада в тази група, както и IPV6 адресите, тъй като те са частично определени от хоста. Освен ако органът не може да гарантира, че IP адресът не произхожда от крайното устройство на потребител или абонат, той трябва да предприеме всички стъпки съгласно член 5, параграф 3 от Директивата.

[28] Това е допълнително и независимо от използването и функцията на IP адреса за установяване и пренасяне или предаване на основни технически комуникации или от факта, че това може да бъдат или да не бъдат лични данни (по отношение на анализа на защитата на личните данни в областта на електронните комуникации това е „информация“).

[29] Доставчиците на интернет услуги използват мрежови адреси (NAT) с преносен клас или CGNAT, за да се увеличи до максимум използването на ограничено пространство на IP адрес. Няколко абонати се групират в един и същ публичен IP адрес.

56. Въпреки че в настоящите насоки не се анализира прилагането на изключенията от задължението за получаване на съгласие, предвидено в член 5, параграф 3 от ДПНЕК, е важно отново да се припомни, че приложимостта на този член не означава, че трябва систематично да се получава съгласие. Поради това ЕКЗД напомня, че във всеки случай ще трябва да се прецени дали е необходимо съгласие или може да се приложи освобождаване съгласно член 5, параграф 3 от ДПНЕК[30].

3.4 Периодично и опосредствано отчитане на интернет на нещата

57. Устройствата за IoT (интернет на нещата) произвеждат информация непрекъснато във времето, например чрез датчици, вградени в устройството, които може да бъдат или да не бъдат предварително локално обработени. В много случаи информацията се предоставя на отдалечен сървър, но начините на събиране могат да бъдат различни.

58. Някои устройства за интернет на нещата имат пряка връзка с обществена комуникационна мрежа с клетъчна SIM карта. Други могат да имат непряка връзка с обществена съобщителна мрежа, например чрез използване на WIFI или предаване на информация на друго устройство чрез връзка от типа „точка към точка“ (например чрез Bluetooth). Другото устройство може да бъде например смартфон или специален портал за достъп, който може да обработва или да не обработва предварително информацията, преди да я изпрати към сървъра.

59. Производителят може да инструктира устройствата за интернет на нещата винаги да предават събраната информация, но все пак първо да я кешират локално, например докато се появи връзка.

60. Във всеки случай самото устройство за интернет на нещата, когато е свързано (пряко или непряко) с обществена съобщителна мрежа, се счита за крайно оборудване. Фактът, че информацията се излъчва в реално време или е кеширана за периодично докладване, не променя естеството на тази информация. И в двата случая се прилага член 5, параграф 3 от ДПНЕК, тъй като чрез инструкцията на кода на устройството за интернет на нещата да изпраща динамично съхраняваните данни на отдалечения сървър е налице „получаване на достъп“.

3.5 Уникален идентификатор

61. Общ инструмент, използван от компаниите, е понятието „универсални идентификатори“ или „постоянни идентификатори“. Тези идентификатори могат да бъдат извлечени от трайни лични данни (име и фамилия, електронна поща, телефонен номер и др.), които се хешират на устройството на потребителя, събират се и споделят между няколко администратори с цел уникално идентифициране на дадено лице чрез различни набори от данни (данни за използването, събрани чрез използването на уебсайт или приложение, данни за управление на връзките с клиентите (CRM), свързани с онлайн или офлайн покупка или абонамент и др.). В уебсайтовете постоянните лични данни обикновено се получават във връзка с удостоверяване на автентичността или абониране за бюлетини.

62. Както беше посочено по-горе, фактът, че информацията се въвежда от потребителя, не изключва прилагането на член 5, параграф 3 от ДПНЕК по отношение на съхранението, тъй като тази информация се съхранява временно в крайното оборудване, преди да бъде събрана.

[30] В Становище 9/2014 на РГ 29 са дадени някои примери, когато може да не е необходимо съгласие.

63. Във връзка със събирането на „уникалния идентификатор“ на уебсайтове или мобилни приложения, субектът, който събира информацията, инструктира браузъра (чрез разпространение на код от страна на клиента) да изпрати тази информация. Поради това е налице „получаване на достъп“ и се прилага член 5, параграф 3 от ДПНЕК.