



17/BG

WP 247

**Становище 01/2017 относно  
предложението за Регламент за неприкосновеността на личния живот и  
електронните съобщения (2002/58/ЕО)**

**Прието на 4 април 2017 година**

Тази работна група е създадена в съответствие с член 29 от Директива 95/46/ЕО. Тя е независим европейски консултативен орган относно защитата на личните данни и неприкосновеността на личния живот. Нейните задачи са описани в член 30 от Директива 95/46/ЕО и член 15 от Директива 2002/58/ЕО.

Секретариатът е осигурен от Дирекция С (Основни права и върховенство на закона) на Генерална дирекция „Правосъдие и потребители“ на Европейската комисия, В-1049 Brussels, Belgium, Офис № MO-59 05/035.

Уебсайт: [http://ec.europa.eu/justice/data-protection/index\\_en.htm](http://ec.europa.eu/justice/data-protection/index_en.htm)

**РАБОТНАТА ГРУПА ЗА ЗАЩИТА НА ЛИЦАТА ПРИ ОБРАБОТВАНЕТО НА ЛИЧНИ ДАННИ**

създадена с Директива 95/46/ЕО на Европейския парламент и на Съвета от 24 октомври 1995 г.,

като взе предвид членове 29 и 30 от нея,

като взе предвид Правилника за дейността си,

**ПРИЕ НАСТОЯЩОТО СТАНОВИЩЕ:**

## РЕЗЮМЕ

Работната група приветства предложението на Европейската комисия от 10 януари 2017 г. за Регламент за неприкосновеността на личния живот и електронните съобщения. Работната група приветства **избора на регламент** като регулаторен инструмент. По този начин се гарантира, че правилата са еднакви навсякъде в ЕС и се осигурява яснота както за надзорните органи, така и за организациите. Освен това по този начин се спомага за осигуряването на съгласуваност с Общия регламент относно защитата на данните (ОРЗД). Тази съгласуваност допълнително се подкрепя от решението **органът, отговорен за наблюдението на спазването на ОРЗД**, да отговаря и за изпълнението на правилата за неприкосновеността на личния живот и електронните съобщения.

Същевременно изборът за (запазване на) **допълващ правен инструмент** е положителен. Защитата на поверителните съобщения и крайните устройства има специфични особености, които не са разгледани в ОРЗД. Поради това са необходими допълнителни разпоредби по отношение на тези видове услуги, за да се гарантира подходяща защита на основното право на неприкосновеност на личния живот и поверителност на съобщенията, включително поверителност на крайните устройства. В това отношение работната група категорично подкрепя възприетия в предложениия регламент **принципен подход за широко формулирани забрани и тясно формулирани изключения**, както и **целевото прилагане на понятието за съгласие**.

Работната група приветства разширяването на обхвата на предложениия регламент, така че в него да се включат **доставчици на „over-the-top“ („OTT“) услуги**, тъй като тези услуги са функционално равностойни на по-традиционните средства за комуникация и поради това разполагат със сходен потенциал да окажат въздействие върху неприкосновеността на личния живот и правото на тайна на съобщенията на хората в ЕС. Друга положителна черта е, че предложениият регламент очевидно обхваща **съдържанието и свързаните с него метаданни** и че в него се признава, че **метаданните могат да разкрият много чувствителни данни**.

При все това Работната група също така отбелязва 4 точки, които пораждат **сериозна тревога**. По отношение на **проследяването на местонахождението на крайните устройства; условията, при които се позволява анализ на съдържанието и метаданните; настройките по подразбиране на крайните устройства и софтуера, както и по отношение на стените за проследяване** предложениият регламент би довел до понижаване на нивото на защита, установено в съответствие с ОРЗД. В настоящото становище Работната група отправя конкретни предложения, с които да се гарантира, че Регламентът за неприкосновеността на личния живот и електронните съобщения ще осигури същото или по-високо ниво на защита, подходящо за чувствителното естество на данни от съобщения (както съдържание, така и метаданни).

Що се отнася до **проследяването чрез WiFi**, в зависимост от обстоятелствата и целта на събирането на данни такова проследяване съгласно ОРЗД вероятно или ще подлежи на съгласие, или ще може да се извършва само ако събираните лични данни са анонимизирани. В последния случай трябва да бъдат изпълнени следните 4 условия: целта, с която се събират данни от крайното устройство, е ограничена само до

статистическо преброяване, проследяването е ограничено във времето и пространството до степента, която е строго необходима за тази цел, данните ще бъдат заличени или анонимизирани незабавно след обработването и съществуват ефективни възможности за отказ. Европейската комисия се приканва да насърчи технически стандарт, съгласно който мобилните устройства автоматично да сигнализируют за възражение срещу такова проследяване.

Що се отнася до **анализа на съдържанието и метаданните**, отправната точка следва да бъде, че е забранено да се обработват данни от съобщения без съгласието на всички крайни ползватели (изпращачи и получатели). За да се даде възможност на доставчиците да предоставят услугите, изрично поискани от ползвателя, като например функция за търсене и индексирание или услуги „от текст към говор“, следва да бъде въведено изключение за лични нужди, свързано с обработването на съдържание и метаданни за изцяло личните цели на самия ползвател.

Що се отнася до **съгласието за проследяване**, Работната група призовава за изрична забрана на стените за проследяване, тоест избори от вида „приемаш или се отказваш“, които принуждават ползвателите да се съгласят да бъдат проследявани, ако искат достъп до услугата.

Не на последно място, Работната група препоръчва крайните устройства и софтуерът **по подразбиране да бъдат настроени за защита на неприкосновеността на личния живот** и да предлагат ясни варианти на ползвателите за потвърждаване или промяна на тези настройки по подразбиране по време на инсталацията. Настройките трябва да бъдат лесно достъпни по време на използването. Ползвателите трябва да имат възможност да посочат конкретно съгласие чрез настройките на своя браузър. Предпочитанията във връзка с неприкосновеността на личния живот не следва да се ограничават до вмешателство от трети страни или до използване на бисквитки. Работната група настоятелно препоръчва спазването на стандарта „Не проследявай“ да стане задължително.

Работната група също така установи други поводи за опасения, свързани например с обхвата, защитата на крайните устройства и директния маркетинг. Не на последно място, Работната група определи някои въпроси, които трябва да се пояснят, за да се защитят по-добре крайните ползватели и да се постигне по-голяма правна сигурност за всички участващи заинтересовани страни.

## СЪДЪРЖАНИЕ

<b>1. ВЪВЕДЕНИЕ .....</b>	<b>6</b>
<b>2. ПОЛОЖИТЕЛНИ АСПЕКТИ НА ПРЕДЛОЖЕНИЯ РЕГЛАМЕНТ .....</b>	<b>6</b>
<i>Хармонизация на равнище ЕС, съгласуване на глобите и изключително прилагане от органите по защита на данните .....</i>	
<i>Разширяване на обхвата в сравнение с Директивата за правото на неприкосновеност на личния живот и електронни комуникации .....</i>	<i>8</i>
<i>Целево прилагане на понятието за съгласие .....</i>	<i>10</i>
<b>3. ПОВОДИ ЗА СЕРИОЗНИ ОПАСЕНИЯ .....</b>	<b>11</b>
<i>Защитата съгласно ОРЗД се подронва от предложения регламент .....</i>	<i>11</i>
<b>4. ДРУГИ ПОВОДИ ЗА ОПАСЕНИЯ .....</b>	<b>18</b>
<i>Териториалният и материалният обхват трябва да бъде разширен .....</i>	<i>18</i>
<i>Защитата на крайните устройства трябва да бъде засилена .....</i>	<i>19</i>
<i>Директен маркетинг .....</i>	<i>24</i>
<i>График .....</i>	<i>27</i>
<i>Други опасения .....</i>	<i>27</i>
<b>5. ПРЕДЛОЖЕНИЯ ЗА ПОЯСНЕНИЯ С ЦЕЛ ОСИГУРЯВАНЕ НА ПРАВНА СИГУРНОСТ .....</b>	<b>31</b>
<i>Пояснения относно обхвата .....</i>	<i>31</i>
<i>Пояснения относно понятието за съгласие и прилагането му .....</i>	<i>34</i>
<i>Пояснения относно местонахождението и други метаданни .....</i>	<i>36</i>
<i>Пояснения относно нежелани съобщения .....</i>	<i>38</i>
<i>Пояснения относно прилагането на инструменти за основните права .....</i>	<i>39</i>
<i>Други пояснения .....</i>	<i>40</i>

## 1. ВЪВЕДЕНИЕ

1. Работната група за защита на личните данни по член 29 (Работната група или РГ29) приветства предложението за регламент на Европейската комисия (ЕК) за неприкосновеността на личния живот и електронните съобщения (предложения регламент, предложен регламент или регламент за неприкосновеността на личния живот и електронните съобщения)<sup>1</sup>, чиято цел е да замени Директивата за правото на неприкосновеност на личния живот и електронни комуникации (ДПНЛЖЕК)<sup>2</sup>.
2. Редица аспекти на предложения регламент са положителни и Европейската комисия направи важна стъпка с неговото представяне. Предложеният регламент обаче може да бъде подобрен допълнително. По този начин ще се спомогне не само за по-добра защита на крайните ползватели, но и ще се постигне по-голяма правна сигурност за всички участващи заинтересовани страни.
3. Поради това Работната група желае да изтъкне няколко повода за опасение и да отправи препоръки за пояснения, които да бъдат разгледани от Европейския парламент и Съвета на министрите, когато обсъждат предложения регламент. В настоящото становище първо ще бъдат разгледани положителните аспекти на предложения регламент и след това ще бъдат изтъкнати поводите за опасение и въпросите, които се нуждаят от пояснение.

## 2. ПОЛОЖИТЕЛНИ АСПЕКТИ НА ПРЕДЛОЖЕНИЯ РЕГЛАМЕНТ

*ХАРМОНИЗАЦИЯ НА РАВНИЩЕ ЕС, СЪГЛАСУВАНЕ НА ГЛОБИТЕ И ИЗКЛЮЧИТЕЛНО ПРИЛАГАНЕ ОТ ОРГАНИТЕ ПО ЗАЩИТА НА ДАННИТЕ*

4. Работната група приветства **избора на регламент като регулаторен инструмент**. По този начин се гарантира, че правилата са еднакви навсякъде в ЕС (с някои изключения, които ще бъдат обсъдени по-долу). Така се осигурява яснота както за надзорните органи, така и за организациите. Освен това предвид ключовата роля на Общия регламент относно защитата на данните (ОРЗД)<sup>3</sup> за

---

<sup>1</sup> Предложение за регламент на Европейския парламент и на Съвета относно зачитането на личния живот и защитата на личните данни в електронните съобщения и за отмяна на Директива 2002/58/ЕО (Регламент за неприкосновеността на личния живот и електронните съобщения), 2017/0003 (COD), url: [http://ec.europa.eu/newsroom/dae/document.cfm?doc\\_id=41241](http://ec.europa.eu/newsroom/dae/document.cfm?doc_id=41241).

<sup>2</sup> 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 (Директива за правото на неприкосновеност на личния живот и електронни комуникации), ОВ L 201, 31.7.2002 г., стр. 37—47, url: <http://eur-lex.europa.eu/legal-content/BG/TXT/?uri=celex:32002L0058>.

<sup>3</sup> Регламент (ЕС) 2016/679 на Европейския парламент и на Съвета от 27 април 2016 г. относно защитата на физическите лица във връзка с обработването на лични данни и относно свободното движение на такива данни и за отмяна на Директива 95/46/ЕО (Общ регламент относно защитата на данните), ОВ L 119/1, 4.5.2016 г., стр. 1—88, url: <http://eur-lex.europa.eu/legal-content/BG/TXT/?uri=CELEX:32016R0679>.

предложения регламент, така се спомага да се гарантира съгласуваност между двата инструмента. Същевременно **изборът за (запазване на) допълващ правен инструмент** е положителен. Защитата на поверителните съобщения и крайните устройства има специфични особености, които не са разгледани в ОРЗД. Поради това са необходими допълнителни разпоредби по отношение на тези видове услуги, за да се гарантира подходяща защита на това основно право. В този контекст Работната група също така **подкрепя възприетия в предложения регламент принципен подход за широко формулирани забрани и тясно формулирани изключения** и счита, че следва да се избягва въвеждането на общо формулирани изключения по подобие на член 6 от ОРЗД и по-специално на член 6, буква е) от ОРЗД (въз основа на легитимни интереси).

5. **Прилагането на тези правила от един и същ орган, отговорен за наблюдението на спазването на ОРЗД**, допълнително ще засили съгласуваността между двата инструмента. С оглед на връзката между защитата на личните данни и защитата на поверителните съобщения и крайните устройства е от полза прилагането на разпоредбите съгласно предложения регламент да бъде възложено на същия надзорен орган, който отговаря за прилагането на ОРЗД (съображение 38 и член 18 от предложения регламент). Освен това в съдебната практика на Съда на Европейския съюз (Съда на ЕС)<sup>4</sup> се потвърждава, че е изключително важно надзорният орган да бъде независим, както е посочено в член 7 от Хартата. В практически план обаче това би довело до значителна по обем допълнителна работа за органите по защита на данните (ОЗД), без да има гаранция, че тази задача ще бъде изпълнена, ако не бъдат отпуснати допълнителни средства. Поради това ОЗД приветстват съображение 38 от предложения регламент, в което се подчертава, че на всеки надзорен орган следва да бъдат предоставени допълнителни финансови и човешки ресурси, помещения и инфраструктура, които са необходими за ефективното изпълнение на задачите съгласно новия регламент. Приветства се и фактът, че член 18, параграф 2 съдържа правното основание за сътрудничество между надзорните органи по предложения регламент и националните регулаторни органи по предложената директива за установяване на Европейски кодекс за електронни съобщения („ЕКЕС“)<sup>5</sup>.
6. С оглед на тясната връзка между предложения регламент и ОРЗД **съгласуването на глобите съгласно предложения регламент и ОРЗД** също се приветства. Дейностите, които попадат в обхвата на предложения регламент, са изключително чувствителни и, наред с другото, включват вмешателството в поверителните съобщения и крайните устройства. Размерът на глобите следва да бъде пропорционален спрямо този чувствителен контекст. Този контекст е и

---

<sup>4</sup> Вж. например решение на Съда от 6 октомври 2015 г., C-362/14 (*Safe Harbour*), точка 41 и решение на Съда от 21 декември 2016 г., C-203/15 и C-698/15 (*Tele2/Watson*), точка 123.

<sup>5</sup> Предложение за Директива на Европейския парламент и на Съвета за установяване на Европейски кодекс за електронни съобщения (преработена), 2016/0288 (COD), 12.10.2016 г., url: [http://eur-lex.europa.eu/legal-content/BG/ALL/?uri=comnat:COM\\_2016\\_0590\\_FIN](http://eur-lex.europa.eu/legal-content/BG/ALL/?uri=comnat:COM_2016_0590_FIN).

причината, поради която е важно да се постигне хармонизация навсякъде в ЕС, така че да се осигури едно и също високо ниво на защита в целия регион. В член 23 от предложения регламент се предвиждат ефективни глоби при нарушаване на неговите разпоредби, като техният размер е подобен на размера на глобите, определени за нарушаване на разпоредбите на ОРЗД, с изключение на някои аспекти (вж. точка 38).

7. Приветства се и фактът, че от този законодателен акт **отпаднаха някои конкретни правила за уведомление при нарушаването на сигурността на данните**, тъй като така се предотвратява ненужно припокриване с въведените в ОРЗД изисквания при нарушаване на сигурността на данните.
8. Освен това се **приветства фактът, че понастоящем е поставен акцент върху осигуряването на еднаква защита на всички крайни ползватели**, тъй като от предложения регламент отпадна понятието за разграничение между „абонати“ и други ползватели на електронни съобщителни услуги.

*РАЗШИРЯВАНЕ НА ОБХВАТА В СРАВНЕНИЕ С ДИРЕКТИВАТА ЗА ПРАВОТО НА НЕПРИКОСНОВЕНОСТ НА ЛИЧНИЯ ЖИВОТ И ЕЛЕКТРОННИ КОМУНИКАЦИИ*

9. Работната група приветства **разширяването на обхвата на предложения регламент, така че в него да се включат доставчици на „over-the-top“ („ОТТ“) услуги**, тъй като тези услуги са функционално равностойни на по-традиционните средства за комуникация и поради това разполагат със сходен потенциал да оказват въздействие върху неприкосновеността на личния живот и правото на тайна на съобщенията на гражданите на ЕС. По-специално Работната група приветства факта, че понастоящем всички категории на ОТТ услуги (ОТТ0, ОТТ1 и някои ОТТ2)<sup>6</sup> попадат в обхвата на регламента, тъй като той обхваща не само традиционните средства за комуникация (ОТТ0), но и функционално равностойни услуги (ОТТ1), както е посочено в член 8, параграф 1, буква в) от предложения регламент. Друга положителна черта е, че в допълнение към определенията по ЕКЕС са включени и някои ОТТ2, когато те осигуряват спомагателна междуличностна и интерактивна комуникация, неразделно свързана с тяхната услуга, като например в игри, приложения за срещи или уебсайтове за отзиви (член 4, параграф 2 от предложения регламент). По подобен начин се приветства **пояснението, че защитата обхваща и предаването на съобщения между машини**. В съображение 12 се посочва ясно, че устройствата, които общуват помежду си, попадат в обхвата на защитата, осигурена съгласно предложения регламент. Това е желателно, тъй

---

<sup>6</sup> За по-подробно обяснение на тези понятия вж. Служба на Органа на европейските регулатори в областта на електронните съобщения (BEREC), *Report on OTT Services (Доклад относно ОТТ услугите)*, BoR (16) 35, 29 януари 2016 г., стр. 15 и 16, url:

[http://berec.europa.eu/eng/document\\_register/subject\\_matter/berec/reports/5751-berec-report-on-ott-services](http://berec.europa.eu/eng/document_register/subject_matter/berec/reports/5751-berec-report-on-ott-services).

Освен това следва да се отбележи коментарът в доклада, че категориите имат предназначение на понятия за използване в обсъждането във връзка с прегледа, а не на правни понятия.



като такива съобщения често съдържат информация, която е защитена от правото на неприкосновеност на личния живот. При все това приложимостта би могла да се поясни (вж. точка 40, буква з).

10. Друга положителна черта е, че **предложеният регламент ясно обхваща както съдържанието, така и свързаните с него метаданни**. От съображение 14 става ясно, че определението за „данни от електронни съобщения“ в член 4, параграф 3, буква а) е предназначено да бъде достатъчно широко, за да може да обхване *цялото* съдържание и свързаните с него метаданни, независимо например от средствата за пренос на сигналите. При все това в точка 39 Работната група изтъква като повод за опасение обстоятелството, че сегашното определение за „данни от електронни съобщения“ продължава да бъде предмет на дискусии. В съответствие с това разширяване на обхвата Работната група счита за изключително важно допълнение **признанието, че метаданните могат да разкрият много чувствителни данни** (вж. точка 2.2 от обяснителния меморандум; съображение 2). Работната група приветства факта, че по този начин Европейската комисия включва в предложението съображенията на Съда на ЕС от решенията по делата *Digital Rights Ireland* и *Tele2/Watson*. РГ29 също така оценява **потвърждението, че анализът на съдържание представлява обработване с висок риск**. В съображение 19 и член 6, параграф 3, буква б) е установена логичната правна презумпция, че сканирането на съдържание представлява обработване с висок риск съгласно член 35 от ОРЗД и очевидно винаги изисква предварителна консултация с (водещия) орган по защита на данните, независимо дали съществува висок остатъчен риск. Същевременно Работната група изразява опасения относно обхвата на определението за „метаданни“ и факта, че анализът на метаданните не подлежи на същото изискване за задължителна ОВЗД (вж. точки 33 и 46).
11. Освен това се приветства фактът, че продължава да се **признава значението на анонимизирането**. В Директивата за правото на неприкосновеност на личния живот и електронни комуникации мерките за анонимизиране вече играеха роля за гарантиране на съвместимостта (например член 6, параграф 1 от Директивата за правото на неприкосновеност на личния живот и електронни комуникации, който предвижда, че данните за трафик трябва да бъдат изтрети или да се направят анонимни, когато не са необходими повече за целите на предаване на съобщение). В член 6, параграф 2, буква в) и член 6, параграф 3, буква б) от предложения регламент се позволява изключение от забраната за обработване на метаданни и съдържание въз основа на съгласие, при условие че тези цели *„не могат да бъдат постигнати чрез обработване на анонимизирана информация“*. Изискването на такива мерки за защита на неприкосновеността на личния живот в допълнение към искането на съгласие от ползвателите защитава тези ползватели от незаконно обработване. Същевременно с това обаче Работната група изразява сериозни опасения, че няма да се изисква приемането на такива техники за анонимизиране, когато се проследява местонахождението на ползвателите чрез техните мобилни устройства (вж. точка 17). Освен това, дори ако бъдат въведени мерки за анонимизиране, доставчиците следва винаги да извършват оценка на въздействието върху защитата на данните (ОВЗД) (вж. точки 33 и 46), като Работната група

призовава за допълнително задължение да се оповестява публично начинът на анонимизиране и агрегиране на данните (вж. точка 42, буква б).

12. Друга положителна черта е **широката формулировка на защитата на крайните устройства**. В съображение 20 и член 8 се посочва, че не е от значение каква технология се използва за осъществяване на достъп до крайното устройство: всяко вмешателство в крайното устройство, включително използването на неговия капацитет за обработка, изисква съгласието на крайния ползвател (с някои изключения). Полезно е, че ЕК потвърди, че създаването на цифрови отпечатъци на устройства е обхванато от тази разпоредба. Освен това Работната група приветства факта, че неспазването от трети страни на предпочитанията, посочени в **настройките на браузъра** на дадено лице, **води до принудително изпълнение**, както е описано в съображение 22. Това е полезно в ситуации, в които трета страна (например рекламна мрежа) не зачита тези настройки. Това обаче следва да бъде посочено и в съответна разпоредба от предложения регламент.
13. На последно място се приветства фактът, че в **обхвата на предложения регламент** продължават да се **включват юридически лица** (вж. точка 2.2 от обяснителния меморандум; съображения 3, 33 и 42; членове 1 и 15 и член 16, параграф 5). Това вече е така съгласно Директивата за правото на неприкосновеност на личния живот и електронни комуникации, но е полезно специално да се подчертае, тъй като органите по защита на данните ще бъдат натоварени с прилагането на новите правила. Това позволява на органите по защита на данните да предприемат действия в случаите, когато юридически лица са обект на нарушение, например когато корпорации получават нежелани съобщения или съобщенията им тайно се наблюдават. При все това Работната група също така отбелязва като повод за опасение факта, че не е ясно как се прилага изискването за съгласие по отношение на юридическите лица (вж. точка 41, буква а) и не е ясно какво се има предвид под „законните интереси“ на юридическите лица при директен маркетинг (вж. точка 43, буква в).

#### *ЦЕЛЕВО ПРИЛАГАНЕ НА ПОНЯТИЕТО ЗА СЪГЛАСИЕ*

14. Работната група приветства още една категория подобрения, свързани с прилагането и тълкуването на понятието за съгласие. На първо място се приветства **пояснението, че услугите за достъп до интернет и за (мобилна) телефония представляват основни услуги и доставчиците на тези услуги не могат да „принуждават“ своите клиенти да се съгласяват с обработване на данни, което не е нужно за предоставянето на самата основна услуга**. По-специално в съображение 18 се отбелязва, че услугите за базов широколентов достъп до интернет и гласови съобщения следва да се разглеждат като основни услуги, което означава, че предвид зависимостта на хората от достъп до такива услуги съгласието за обработването на данните от техните съобщения не може да бъде валидно за такива допълнителни цели (например обработване за рекламни или маркетингови цели). Същевременно Работната група изразява загриженост, че това пояснение е твърде ограничено. Услугите от определени доставчици на ОТТ услуги също могат да се считат за основни услуги и в

Регламента за неприкосновеността на личния живот и електронните съобщения следва също така специално да се забраняват избори от вида „приемаш или се отказваш“ в други обстоятелства (вж. точка 20).

15. Освен това е положителен фактът, че е **хармонизирано изискването за съгласие във връзка с включването на личните данни на физически лица в указатели**. Съгласно член 15 от предложения регламент обработването на данни в обществено достъпни указатели се позволява само със съгласието на физическите лица и при наличие на възможност за възражение, когато става въпрос за юридически лица. Това е обяснено по-подробно в съображение 31, където се отбелязва, че това съгласие трябва да бъде конкретно по отношение на конкретните категории лични данни, които ще бъдат включени в указателя. При все това Работната група отбелязва като повод за опасение, че в предложения регламент би могло да се посочи по-ясно, че ще се изисква конкретно отделно съгласие за търсене и за обратно търсене (вж. точка 37).
16. Оценява се положително и **новото целево изключение за вмешателство в крайните устройства, при което не се нарушава неприкосновеността на личния живот**. Според RG29 е полезно, че в предложения регламент се пояснява, че забраната не се прилага към измерването на трафик към уебсайтове (при тясно формулираното изключение, че това измерване се извършва от доставчика на услугата на информационното общество, поискана от крайния ползвател, вж. член 8, параграф 1, буква г) от предложения регламент). Вж. също така съображение 21. При все това Работната група предлага да се използва по-неутрално от гледна точка на технологията определение и да се поясни приложимостта на това изключение (вж. точка 25).

### **3. ПОВОДИ ЗА СЕРИОЗНИ ОПАСЕНИЯ**

#### *ЗАЩИТАТА СЪГЛАСНО ОРЗД СЕ ПОДРОНВА ОТ ПРЕДЛОЖЕНИЯ РЕГЛАМЕНТ*

Както е посочено по-горе, в предложения регламент съществуват редица ключови подобрения. Налице са обаче и поводи за опасения с различна степен на тежест. В настоящия раздел Работната група обсъжда четирите проблема, по отношение на които изразява **сериозно безпокойство**. Това са разпоредби, които **подронват нивото на защита, осигурено от ОРЗД**:

17. Установените в Регламента задължения във връзка с проследяването на местонахождението на крайните устройства следва да отговарят на изискванията по ОРЗД. Съгласно член 8, параграф 2, буква б) от предложения регламент за събирането на информация, изпратена от крайно устройство, се изисква само показването на съобщение и въвеждането на мерки за сигурност. В член 8, параграф 2, буква б) също така се отбелязва, че лицето, отговарящо за това събиране, трябва да съобщи за всички мерки, които крайният ползвател може да предприеме, за да спре или сведе до минимум събирането. По този начин член 8, параграф 2, буква б) създава впечатлението, че организациите могат да събират информация, изпратена от крайни устройства, за да проследяват физическото движение на отделни лица (като например „проследяване чрез WiFi“ или „проследяване чрез Bluetooth“) без съгласието на съответното лице. Страната, която събира тези данни, изглежда би могла да спази изискването посредством съобщение, с което ползвателите се информират да изключат своите устройства, когато не желаят да бъдат следени. Такъв подход би бил в разрез с една от основните цели на политиката на Европейската комисия в областта на далекосъобщенията — осигуряване на високоскоростна мобилна връзка с интернет със силна защита на неприкосновеността на личния живот и ниски разходи за всички европейски граждани в трансграничен план.

Освен това с предложения регламент не се определят ясни ограничения по отношение на обхвата на събирането на данни или последващите дейности по обработване. В този контекст следва да се отбележи, че тези MAC адреси представляват лични данни дори след въвеждането на мерки за сигурността, като например хеширане. Без определянето на допълнителни изисквания или ограничения нивото на защита на тези лични данни съгласно предложения регламент е значително по-ниско в сравнение с ОРЗД, съгласно който такова проследяване трябва да бъде добросъвестно и законосъобразно, както и прозрачно. Освен това в съображение 25 безполезно се отбелязва, че някои от функциите за проследяване чрез WiFi не водят до високи рискове за неприкосновеността, докато други — например следенето на лица за определени периоди от време — водят. Макар че Работната група оценява признанието, че втората група функции поражда високи рискове за неприкосновеността, не е от полза да се заключи предварително, че определени други функции не поражда такъв риск, без да се извърши допълнителна оценка на обстоятелствата и пропорционалността на обработването. Следва да бъде извършена такава оценка, като се вземат предвид следните условия по отношение на неанонимизираното проследяване чрез Wifi.

В зависимост от обстоятелствата и целите на събирането на данни проследяването съгласно ОРЗД вероятно или ще подлежи на съгласие, или ще може да се извършва само ако събираните лични данни са анонимизирани. За предпочитане е анонимизирането да се извършва непосредствено след събирането на данните. Ако не е възможно да се извърши незабавно анонимизиране с оглед на целите, за които са събрани данните, тези данни могат да бъдат обработени в рамките на определен период, през който не са анонимизирани, само при следните условия: i) целта, с която се събират данни,

трябва да бъде ограничена само до статистическо преброяване (вж. примерите по-долу), ii) проследяването е ограничено във времето и пространството до степента, която е строго необходима за тази цел, iii) данните се заличават или анонимизират незабавно след това и iv) трябва да съществуват ефективни възможности за отказ. Разбира се, администраторите при всички обстоятелства трябва да спазват изискването за предоставяне на подходяща информация.

Работната група изразява опасения, че потенциалното предлагане на възможност за индивидуален отказ по отношение на всяка организация, която събира такива данни, би довело до неприемлива тежест за гражданите с оглед на увеличеното разгръщане на такива технологии за проследяване от организации както от частния, така и от публичния сектор. Поради това Работната група призовава европейския законодател да насърчи разработването на технически стандарти, съгласно които устройствата автоматично да сигнализират за възражение срещу такова проследяване, и да гарантира, че съобразяването с тези сигнали подлежи на принудително изпълнение.

Например съгласно ОРЗД вероятно ще се изисква съгласие, когато администратор събира и съхранява (WiFi или Bluetooth) MAC адреси на устройства, които могат да бъдат непряко идентифицирани, и изчислява местонахождението на ползвателя, за да следи неговото местонахождение за определени периоди от време, например между множество магазини. Такъв е случаят по-специално, когато такова проследяване се извършва в публични зони, където ползвателите основателно очакват да не бъдат идентифицирани или следени, но където въпреки това се събират MAC адресите на преминаващите хора. Такова съгласие може да бъде получено например посредством приложение, което приканва ползвателите да разрешат следене на тяхното местонахождение в конкретни зони в замяна на търговски предложения, посредством предлагане на точки за регистрация на определени места или посредством модул за изразяване на съгласие на места с WiFi точки за достъп.

На администраторите на данни може да бъде позволено да обработват информацията, изпратена от крайното устройство, с цел проследяване на физическото движение без съгласието на съответното лице само в ограничен брой случаи. Например такъв може да бъде случаят при определяне на броя на клиентите на конкретно място или при събиране на изпратените данни от двете страни на пункт за проверка за сигурност, за да се определи времето за чакане. И в двата примера обаче данните трябва да бъдат заличени или анонимизирани непосредствено след изпълнението на статистическата цел. Това означава, че MAC адресите на устройствата на посетителите на дадено място, като например магазин, трябва да бъдат анонимизирани непосредствено след събирането и не се съхраняват постоянно, като по този начин технически се изключва възможността за повторно идентифициране. В примера с определянето на времето за чакане MAC адресите трябва да бъдат заличени или анонимизирани веднага след като данните вече не са необходими за изчисляването на този период (например защото посетителят е минал през проверката за сигурност или защото е напуснал опашката).

Освен това администраторът трябва да спази изискванията за свеждане до минимум на данните (например да не се извършва непрекъснато следене, когато целта е ограничена до работното време на магазина и/или изготвяне на извадка на определен интервал). Администраторите също така трябва да въведат други мерки за смекчаване, за да гарантират, че не се оказва никакво или се оказва много малко въздействие върху правата на неприкосновеност на личния живот на ползвателите, например за да се защити личният живот на хората, които живеят в близост до пункт за събиране на данни.

Решението в член 8, параграф 2 от предложения регламент да се включи само изискване за съобщение е още по-учудващо с оглед на заключението в съображение 20, че информацията, свързана с устройствата на крайните ползватели, може да бъде събирана и от разстояние за целите на идентифициране и проследяване, както и че такова обработване — съгласно предложения регламент — може сериозно да наруши неприкосновеността на личния живот на тези крайни ползватели. Освен това задължението не надхвърля задължението за информиране, което вече е предвидено в членове 13 и 14 от ОРЗД. Сериозното вмешателство в неприкосновеността на личния живот се подсилва допълнително от потенциалния достъп на други лица до събраните данни, като например възможността за правоприлагащите органи да идентифицират крайни ползватели въз основа на съхранените MAC адреси, данните за които се изпратени от техните мобилни устройства.

**18. Трябва да бъдат определени подробно условията, при които се позволява анализ на съдържанието и метаданните.**

В член 6 от предложения регламент се определят различни равнища на защита за метаданните и за съдържанието. РГ29 не подкрепя това разграничение: и двете категории данни са много чувствителни. Поради това метаданните и съдържанието трябва да подлежат на едно и също високо ниво на защита. Следователно отправната точка следва да бъде, че е забранено да се обработват метаданни и съдържание без съгласието на всички крайни ползватели (изпращачи и получатели).

В зависимост от целите обаче може да се позволи известно обработване без съгласие, ако е строго необходимо за тези цели:

- Доставчиците могат да обработват данни от електронни съобщения за целите, посочени в член 6, параграф 1, букви а) и б) и член 6, параграф 2, букви а) и б) от предложения регламент<sup>7</sup>.

---

<sup>7</sup> Що се отнася до необходимостта да се изпълняват задължителни изисквания за качеството на услугата, както е определено в член 6, параграф 2, буква а) от предложения регламент, доставчиците следва да вземат предвид условията, посочени в Регламент (ЕС) 2015/2120 (ЕКЕС), по-специално член 3 и съображения 10 и 13—15. Въз основа на тази разпоредба от доставчиците може да се изисква да обработват данни от съобщения с цел откриване и филтриране на зловерден и шпионски софтуер и може да им бъде позволено да компресират данните.

- Следва да се поясни, че определени техники за откриване/филтриране на нежелани съобщения и за смекчаване на последиците от ботмрежи също могат да бъдат счетени за строго необходими за установяване или прекратяване на неправомерна употреба на електронни съобщителни услуги (член 6, параграф 2, буква б). Що се отнася до филтрирането на нежелани съобщения, на крайните ползватели, които получават нежелани съобщения, следва да бъдат предложени диференцирани възможности за отказ, когато това е технически постижимо.
- Следва да се поясни, че анализът на данните от електронни съобщения за цели, свързани с обслужването на клиенти, също може да бъде обхванат от изключението, че това е „необходимо за фактуриране“ (вж. член 6, параграф 2, буква б). Съответните метаданни могат да се пазят до края на периода, през който фактурата може да бъде законно оспорена или може да се осигури получаване на плащане съгласно националното законодателство. Съответните данни (например URL адреси) могат да се запазват само по искане на крайния ползвател и то само за период, който е строго необходим за решаването на спор във връзка с фактура (което означава, че член 7, параграф 3 следва да бъде съответно изменен).
- Следва да се предостави възможност да се обработват данни от електронни съобщения с цел предоставяне на услуги, изрично поискани от краен ползвател, като например функция за търсене или индексирание по ключови думи, виртуални асистенти, програми „от текст към говор“ и услуги за превод. Това налага въвеждането на изключение за анализа на такива данни за изцяло лични (домашни) нужди, както и за лични нужди във връзка с работата<sup>8</sup>. По този начин това обработване ще бъде възможно без съгласието на всички крайни ползватели, но то ще може да се извършва само със съгласието на крайния ползвател, поискал услугата. Такова конкретно съгласие също така няма да позволи на доставчика да използва тези данни за други цели.

Това означава, че анализът на съдържание и/или метаданни за всички други цели, като например аналитична дейност, профилиране, поведенческа реклама или други цели от (търговска) изгода за доставчика, изисква съгласие от всички крайни ползватели, чиито данни ще бъдат обработени. По отношение на тези ситуации в предложения регламент следва да се поясни, че само по себе си изпращането на електронно писмо или друг вид лично съобщение в резултат от друга услуга на краен потребител, който лично се е съгласил неговото съдържание и метаданни да бъдат обработвани (например при регистрирането за услуга по електронна поща), не представлява валидно съгласие от изпращача.

---

<sup>8</sup> Макар че със съображение 13 от предложения регламент корпоративните мрежи изрично се изключват от неговия обхват, това ново изключение за лични нужди следва също така да обхване използването на услуги за изчисления в облак от служители за нужди, свързани с работата, като например търсенето в тяхната електронна поща.

На последно място следва да се поясни, че обработването на данните на лица, различни от съответните крайни ползватели (например снимка или описание на трето лице в кореспонденция между две лица), също трябва да отговаря на всички съответни разпоредби на ОРЗД.

19. **Крайните устройства и софтуерът трябва по подразбиране да обезкуражават, предотвратяват и забраняват незаконното вмешателство в тях и да предоставят информация относно възможностите.** Макар че предложеният регламент задължава доставчиците на софтуер за осъществяване на електронни съобщения да „предлагат възможност“ да се предотврати ограничена форма на вмешателство в крайното устройство и също така задължава доставчиците на софтуер при инсталиране да изискват от крайния ползвател да се съгласи с една от настройките за неприкосновеност (член 10, параграфи 1 и 2), този избор не представлява *неприкосновеност на личния живот по подразбиране*. Освен това „възможността“ за предотвратяване на определено вмешателство вече съществува и досега не е довела до решаване в достатъчна степен на проблема с незаконното следене. Именно поради това в ОРЗД бе направен съзнателен избор на политиката да се въведат принципите на защита на данните на етапа на проектирането и по подразбиране (член 25 от ОРЗД). Предложеният регламент подронва тези принципи по отношение на данните от съобщения и устройства. Същевременно Директивата за радиосъоръженията 2014/53/ЕС<sup>9</sup> (посочена в съображение 10) предвижда само изключително ограничено задължение за сигурност, като изисква радиосъоръжението да има „вградена защита, за да се осигури, че личните данни и неприкосновеността на личния живот на ползвателя и абоната са защитени“ (член 3, параграф 3, буква д). Това не може да замени специалните настройки за неприкосновеност на личния живот по подразбиране съгласно предложеният регламент. В това отношение също така е полезно да се отбележи, че в проучването на Евробарометър относно правото на неприкосновеност на личния живот и електронните комуникации, публикувано през декември 2016 г., се отбелязва, че „почти седем от всеки десет души (69 %) са напълно съгласни, че настройките по подразбиране на техния браузър следва да предотвратяват споделянето на тяхна информация“<sup>10</sup>. Работната група изразява отделно опасение във връзка с настройките на браузърите и определението за „трети страни“. Вж. точка 24. Освен това следва да се има предвид, че тази разпоредба касае не само браузърите, използвани на компютрите, но обхваща и други видове софтуер, които позволяват осъществяване на съобщения (включително операционни системи, приложения и софтуерни интерфейси за устройства, свързани към т. нар. „интернет на предметите“). В обобщение крайните устройства и софтуерът трябва *по подразбиране* да предлагат настройки за защита на неприкосновеността на личния живот и да насочват

<sup>9</sup> Директива за радиосъоръженията 2014/53/ЕС.

<sup>10</sup> Вж. експресно проучване на Евробарометър № 443, Доклад относно правото на неприкосновеност на личния живот и електронните комуникации (публикуван през декември 2016 г.), стр. 5.



ползвателите през менютата за настройване, ако желаят да се отклонят от тези настройки по подразбиране при инсталирането. Тези менюта за настройване следва винаги да бъдат лесно достъпни при използване. Работната група насърчава европейския законодател да поясни обхвата на член 10 по този въпрос.

20. **Регламентът за неприкосновеността на личния живот и електронните съобщения следва изрично да забранява стените за проследяване**, т.е. практиката, при която се отказва достъп до уебсайт или услуга, освен ако лицето не се съгласи да бъде следено в други уебсайтове или услуги. Както вече бе отбелязано в предходните становища на Работната група относно Директивата за правото на неприкосновеност на личния живот и електронни комуникации<sup>11</sup>, такива подходи от вида „приемаш или се отказваш“ рядко са законни<sup>12</sup>. Когато използването на капацитета за обработка и съхранение на крайното устройство или събирането на информация от крайните устройства на крайните ползватели позволява следенето на дейностите на ползватели за определени периоди от време или в контекста на няколко различни услуги (например различни уебсайтове или приложения), такива дейности по обработване могат сериозно да нарушат неприкосновеността на личния живот на тези ползватели. Предвид фундаменталното значение на интернет за създаването на условия за упражняване на основното право за свобода на изразяване, включително правото на достъп до информация, възможността на физическите лица за онлайн достъп до съдържание не следва да зависи от приемане на следенето на дейностите им на различни устройства и уебсайтове/приложения. Поради това в бъдещия регламент за неприкосновеността на личния живот и електронните съобщения следва да се посочи, че достъпът до съдържание, например в уебсайтове и приложения, не може да бъде обвързан с условие да се приемат дейности по обработване, които нарушават неприкосновеността на личния живот, независимо от използваната технология за проследяване, например бисквитки, създаване на цифрови отпечатъци на устройства, въвеждане на уникални идентификатори или други техники за наблюдение. Необходимостта от тази забрана се подчертава от неотдавнашното проучване на Евробарометър относно правото на неприкосновеност на личния живот и електронните комуникации, в което се отбелязва, че „почти две трети от респондентите заявяват, че е неприемливо техните дейности онлайн да се наблюдават в замяна на неограничен достъп до определен уебсайт (64 %)“.

21. В обобщение по отношение на горепосочените четири точки **следва да се изпълни обещанието предложеният регламент да осигурява същото или по-високо ниво на защита от ОРЗД**. В съображение 5 се констатира просто, че предложеният регламент не понижава нивото на защита, осигурено съгласно ОРЗД. Това обаче не е вярно в сегашния вид на предложения регламент,

<sup>11</sup> Вж. например WP240 (преглед на правото на неприкосновеност на личния живот и електронни комуникации), стр. 16; WP 208 (изключение от изискването за съгласие), стр. 5.

<sup>12</sup> Тази позиция не засяга член 7, параграф 4 от ОРЗД, който също може да предотврати избори от вида „приемаш или се отказваш“ в други ситуации, където това е подходящо.

особено по отношение на проследяването на устройства (точка 17), липсващия принцип за неприкосновеност на личния живот по подразбиране (точка 19) и съгласието (точка 18). Това е от особено значение, тъй като в същото съображение се посочва, че предложеният регламент ще бъде „*lex specialis* по отношение на ОРЗД и ще го конкретизира и допълни по отношение на данните от електронните съобщения, които се определят като лични данни“. Работната група предлага като минимум в текста на Регламента за неприкосновеността на личния живот и електронните съобщения да се поясни, че:

- i) забраните в съответствие с Регламента за неприкосновеността на личния живот и електронните съобщения имат предимство пред разрешенията в съответствие с ОРЗД (например забраната за намеса съгласно член 5 от Регламента за неприкосновеността на личния живот и електронните съобщения има предимство пред правата на доставчиците на електронни съобщителни услуги за по-нататъшно обработване на лични данни съгласно член 5, параграф 1, буква б) и член 6, параграф 4 от ОРЗД);
- ii) когато обработването е позволено съгласно някое от изключенията (включително от изискването за съгласие) от забраните съгласно Регламента за неприкосновеността на личния живот и електронните съобщения, ако това обработване е свързано с лични данни, то все пак трябва да отговаря на всички съответни разпоредби от ОРЗД;
- iii) когато обработването е позволено съгласно някое от изключенията от забраните съгласно Регламента за неприкосновеността на личния живот и електронните съобщения, всяко друго обработване въз основа на ОРЗД се забранява, включително обработването за друга цел въз основа на член 6, параграф 4 от ОРЗД. Това няма да попречи на администраторите да поискат допълнително съгласие за нови операции по обработване. Това също така няма да попречи на законодателите да предвидят допълнителни, ограничени и специфични изключения в Регламента за неприкосновеността на личния живот и електронните съобщения, например позволяващи обработване за научни или статистически цели по силата на член 89 от ОРЗД или за защита на „жизненоважните интереси“ на физически лица съгласно член 6, параграф 1, буква г) от ОРЗД.

Освен това Регламентът за неприкосновеността на личния живот и електронните съобщения следва да се тълкува по начин, който гарантира, че той осигурява поне същото ниво на защита като това, осигурено от ОРЗД, а когато това е целесъобразно — по-високо ниво на защита.

#### **4. ДРУГИ ПОВОДИ ЗА ОПАСЕНИЯ**

В допълнение към горепосочените точки Работната група по член 29 изразява **опасения** по отношение на следните въпроси.

*ТЕРИТОРИАЛНИЯТ И МАТЕРИАЛНИЯТ ОБХВАТ ТРЯБВА ДА БЪДЕ РАЗШИРЕН*

- 22. Определението за „метаданни“ е твърде тясно формулирано.** Понастоящем те са определени в член 4, параграф 3, буква в) като „данни, обработени в електронна

съобщителна мрежа за целите на предаването, разпространението или обmena на съдържание на електронни съобщения“ (подчертаването е добавено). Използването на думата „мрежа“ изглежда предполага, че само данните, генерирани в хода на предоставянето на услуги в „по-долния“ слой на мрежата, се класифицират като „метаданни“. Това би могло да означава, че данните, генерирани при предоставянето на ОТТ услуга, ще бъдат изключени от този обхват. Това не е желателно и вероятно целта не е била такава предвид намерението обхванат на предложениия регламент да се разшири, така че да обхване и доставчиците на ОТТ услуги. За да се реши този проблем, определението за „метаданни на електронни съобщения“ следва да бъде изменено така, че да включва всички данни, които се обработват за целите на предаването, разпространението или обmena на съдържание на електронни съобщения.

23. В допълнение към това опасения поражда и фактът, че **в рамките на териториалния обхват на предложениия регламент по отношение на организации, които не са установени в ЕС, попадат само доставчиците на електронни съобщителни услуги**. Съгласно предложениия регламент, когато доставчикът на електронни съобщителни услуги не е установен в Съюза, той определя писмено свой представител в Съюза (член 3, параграф 2). Освен това в съображение 9 се посочва, че регламентът следва да се прилага към обработване от страна на доставчици на електронни съобщителни услуги, независимо къде се извършва обработването. Работната група приветства това пояснение. При все това, тъй като формулировката е ограничена до доставчици на електронни съобщителни услуги, не е ясно до каква степен този териториален обхват се прилага към други видове страни (например страни, които осъществяват вмешателство в крайното устройство на крайния ползвател или събират информация, изпратена от него, вж. член 3, параграф 1, буква в) и член 8 от предложениия регламент). Поради това Работната група предлага член 3, параграф 2 и член 3, параграф 5 да бъдат изменени, така че да включват доставчиците на обществено достъпни указатели, доставчиците на софтуер, позволяващ електронни съобщения, и лицата, които изпращат съобщения на директния маркетинг или събират (друга) информация, свързана със или съхранявана в терминалните устройства на крайните ползватели, когато техните дейности са насочени към ползватели в ЕС (вж. съображение 8 от предложениия регламент)<sup>13</sup>.

#### *ЗАЩИТАТА НА КРАЙНИТЕ УСТРОЙСТВА ТРЯБВА ДА БЪДЕ ЗАСИЛЕНА*

Друга категория опасения е свързана с недостатъчната защита на крайните устройства, която се осигурява от предложениия регламент.

---

<sup>13</sup> Вж. член 3, параграф 2 от ОРЗД: „Настоящият регламент се прилага за обработването на лични данни на субекти на данни, които се намират в Съюза, от администратор или обработващ лични данни, който не е установен в Съюза, когато дейностите по обработване на данни са свързани със: а) предлагането на стоки или услуги на такива субекти на данни в Съюза, независимо дали от субекта на данни се изисква плащане; или б) наблюдението на тяхното поведение, доколкото това поведение се проявява в рамките на Съюза.“ Това задължение също така би могло да включва изключения, следващи логиката на член 27, параграф 2 от ОРЗД.

24. Първо, **предложеният регламент създава погрешното впечатление, че може да бъде изразено валидно съгласие чрез неспецифични настройки на браузъра**. Работната група отчита съображението, че понастоящем крайните ползватели са претоварени с искания за даване на съгласие (съображение 22). Настройките на браузъра (и друг съпоставим софтуер) изпълняват определена роля за решаването на този проблем. При все това, тъй като общите настройки на браузъра не са предназначени да се прилагат за използването на технология за проследяване в един конкретен случай, те не са подходящи за даване на съгласие в съответствие с член 7 и съображение 32 от ОРЗД (тъй като съгласието не е достатъчно конкретно и информирано).

Крайният ползвател трябва да бъде в състояние да даде отделно съгласие за всеки уебсайт или приложение във връзка с проследяване за различни цели (например споделяне в социалните медии или реклама). Администратор на данни, който е отговорен за няколко уебсайта или приложения, също така може да поиска съгласие за всички други уебсайтове или приложения под негов контрол, при условие че това искане за съгласие се представя отделно.

Освен това администраторът трябва да спазва всички други задължения във връзка със съдържанието, включително задължението да предоставя на ползвателите подходяща информация. За браузърите и администраторите на данни това означава, че съгласието не би било действително, ако те предлагат само варианта „приеми всички бисквитки“, тъй като той не би позволил на ползвателите да дадат необходимото диференцирано съгласие. При все това следва да бъде възможно браузърите да позволяват на ползвателите да направят информиран и съзнателен избор за приемане на всички бисквитки и по този начин да възпрепятстват всички бъдещи искания за конкретно съгласие от уебсайта, който посещават.

Работната група настоятелно препоръчва с Регламента за неприкосновеността на личния живот и електронните съобщения да се въведе задължение браузърите да включват технически механизми, като например стандарта „Не проследявай“, за да се гарантира, че на ползвателите се осигурява реален избор и контрол по отношение на вмешателството в техните устройства<sup>14</sup>.

Като още по-важен елемент Регламентът за неприкосновеността на личния живот и електронните съобщения следва да гарантира, че както изборът по отношение на съхранението на информация на устройството, така и сигналът „Не проследявай“ от браузър се приемат като правно обвързващ израз на съгласие или отказ от всички администратори. Това не засяга евентуални допълнителни насоки от Работната група относно спазването на стандарта „Не проследявай“, наред с другото, с принципа за ограничаване в рамките на целта, когато стандартът бъде финализиран (това е насрочено за края на 2017 г.).

Имплицитните видове съгласие, като например отварянето на уебсайт или придвижването по страницата, не могат да имат предимство пред избори по

---

<sup>14</sup> Вж. следния url: <https://www.w3.org/TR/tracking-compliance/>. В точка 7 се обяснява моделът за изключения и разграничението между изключенията за уебсайт и изключението за цялата мрежа. Точка 6 включва машинночитаемата информация, която администраторите могат да предоставят във връзка с изискването за информиране с цел получаване на съгласие.

отношение на съхранението и сигнала „Не проследявай“. Важна полза от използването на този стандарт е, че той не е ограничен до технологията за проследяване чрез бисквитки, а обхваща и други видове проследяване, като например създаване на цифрови отпечатъци на устройства.

Ако спазването на този стандарт стане задължително, това ще реши и друг проблем с настоящото използване на понятието „трети страни“ в член 10. Уебсайтовете и приложенията обикновено съдържат множество елементи — както на самия уебсайт, така и външни елементи. Освен това в контекста на посещавания уебсайт може да се изпълнява и външен код, когато уебсайтът изпраща обратно съобщение до сървър на трета страна. Може да се въведе проследяваща бисквитка от първа страна, например когато ползвателят посети уебсайта на социална мрежа. Уебсайтът на тази социална мрежа също така би могъл да е трета страна, когато ползвателят посети друг уебсайт, който комуникира с първия. Във всеки от тези случаи, независимо дали става въпрос за „достъп до“ или „съхранение“ на информация на устройството на крайния ползвател, това представлява вмешателство в устройството, за което се изисква съгласие (освен ако не се прилага някое от изключенията). При стандарта „Не проследявай“ този въпрос е решен чрез използването на понятията „изключение за уебсайта“ и „изключение за цялата мрежа“. Поради това с цел да се подобри правната сигурност на всички заинтересовани страни позоваването на „трети страни“ в Регламента за неприкосновеността на личния живот и електронните съобщения следва да бъде променено, така че да обхване всички субекти, с които комуникира устройството (защото съхраняват или осъществяват достъп до информация на устройството).

За да се направи стандартът „Не проследявай“ съвместим с високото ниво на защита на поверителността на съобщенията и защитата на данните, осигурено съгласно Хартата, в Регламента за неприкосновеността на личния живот и електронните съобщения следва да се уточни, че за разлика от исканията за проследяване в конкретен уебсайт, исканията за проследяване в цялата мрежа трябва да се представят отделно и ползвателите следва да бъдат свободни да приемат или отхвърлят такива искания. Освен това, за да се защитят ползвателите срещу чести искания за съгласие, Регламентът за неприкосновеността на личния живот и електронните съобщения следва да гарантира, че отказът да се приеме проследяване в цялата мрежа от страна на конкретна организация (чрез стандарта „Не проследявай“ или чрез отделен черен списък) не позволява на тази организация да отправя допълнителни искания за съгласие поне за 6 месеца. Това правило не възпрепятства организацията да поиска съгласие на собствения си уебсайт (т.е. искане за съгласие за този уебсайт), когато той бъде посетен пряко от ползвателя (т.е. като първа страна). На практика това означава, че например уебсайт за видеоизлъчване, който използва проследяващи бисквитки, може да поиска съгласие, когато ползвателят посети уебсайта, но в рамките на период от 6 месеца не може да поиска отново съгласие, ако ползвателят е отказал да даде съгласие и посещава други уебсайтове, съдържащи видеоматериали, получени от този уебсайт за видеоизлъчване.

25. Освен това **изключението за „измерване на интернет аудиторията“ е формулирано неточно.** В член 8, параграф 1, буква г) от предложения регламент се предвижда изключение за измерване на интернет аудиторията. Първият повод за опасение е, че това понятие не е определено и може да бъде объркано с профилиране на ползвателите. От определението следва да става ясно, че това изключение не може да се използва за никакви цели, свързани с профилиране. Изключението следва да се прилага само към анализа на използването, който е необходим за анализиране на изпълнението на поисканата от ползвателя услуга, но не и към анализ на ползвателя (т.е. на поведението на ползвателите на уебсайт, приложение или устройство, които могат да бъдат идентифицирани). Поради това изключението не може да се използва при обстоятелства, когато данните могат да бъдат свързани с обработвани от доставчика или от други администратори данни на ползватели, които могат да бъдат идентифицирани. Освен това самото описание предполага приложение със съвсем конкретна технология. Поради това понятието „измерване на интернет аудиторията“ следва да бъде преработено по неутрален от гледна точка на технологията начин, така че да включва и подобна аналитична информация за използването, извлечена от приложения, носими устройства и устройства, свързани към „интернет на предметите“.

Работната група предлага да се почерпи вдъхновение от нидерландското изключение, което се прилага, ако е строго необходимо за получаването на информация относно техническото качество или ефективността на предоставена услуга на информационното общество, и не оказва никакво или съвсем ограничено въздействие върху неприкосновеността на личния живот на съответния абонат и/или краен ползвател (вж. член 11.7а, параграф 3, буква б) от нидерландския Закон за далекосъобщенията). При това изключение се отчита фактът, че повечето данни, които се събират чрез анализ на уебсайтове или приложения, все пак представляват лични данни. Това означава, че обработването на тези данни също е обхванато от ОРЗД. Това например предполага, че анализът на използването би могъл да бъде извършен и от външна организация, но само ако:

- i) организацията действа като администратор на данни;
- ii) е сключено споразумение с изпълнител в съответствие с ОРЗД;
- iii) използваната аналитична технология не позволява повторно идентифициране, което, наред с другото, включва анонимизиране на IP адресите на ползвателите;
- iv) конкретните бисквитки или други данни, използвани за анализа, могат да се използват само за този уебсайт, приложение или носимо устройство и не могат да бъдат свързани към други данни, позволяващи идентифициране;
- v) ползвателите имат право на отказ (вж. също така точки 17 и 50 в настоящото становище).

Въпреки че няма да се изисква съгласие, ако са изпълнени тези условия, администраторите все пак трябва да предоставят подходяща информация на

ползвателите, например чрез полетата за обозначаване на статуса на проследяване в стандарта „Не проследявай“<sup>15</sup>.

26. Регламентът за неприкосновеността на личния живот и електронните съобщения **следва да осигури тесни и точно формулирани изключения от изискванията за съгласие**. Формулировката на изключението от изискването за съгласие във връзка с вмешателство в устройства, посочено в член 8, параграф 1, буква в), е почти идентична с настоящата формулировка в член 5, параграф 3 от Директивата за правото на неприкосновеност на личния живот и електронни комуникации — *„строго необходимо, за да може доставчикът да предостави услуга на информационното общество, изрично поискана от абоната или ползвателя.“*, но ключовата думата „строго“ е пропусната без никакво обяснение. Това поражда опасения поради две причини. Първо, разпоредбата в Директивата за правото на неприкосновеност на личния живот и електронни комуникации вече доведе до широко обсъждане на обхвата ѝ между надзорните органи и организациите, а заличаването на думата „строго“ ще понижи допълнително правната сигурност. Това също е повод за опасение, тъй като Работната група вече предостави насоки относно тълкуването на думата „строго“ в този контекст. Работната група предложи следното пояснение в становището относно освобождаването от изискването за съгласие за някои „бисквитки“ (WP 194):

*„Бисквитката“ е необходима с цел на ползвателя (или абоната) да бъде предоставена конкретна функция: ако „бисквитките“ не са активирани, функцията не може да бъде предоставена, и тази функция е била изрично поискана от ползвателя (или абоната) като част от услуга на информационното общество.“*<sup>16</sup>

Освен това Работната група поясни, че:

*„бисквитките“ на трета страна обикновено не са „строго необходими“ за ползвателя, посещаващ даден уебсайт, тъй като тези „бисквитки“ обичайно са свързани с услуга, различна от „изрично поисканата“ от ползвателя услуга*<sup>17</sup>.

Работната група добави, че използването на социални плъгин модули, насочени към лица, които не използват дадена платформа или уебсайт, също не би било сметено за строго необходимо.

Освен това, макар че член 6, параграф 1, буква б) от предложениия регламент позволява обработването на данни от електронни съобщения, ако това е „необходимо“ за целите на сигурността, в съображение 49 от ОРЗД се изисква

<sup>15</sup> Вж.: „Tracking Preference Expression (DNT)“ (Изразяване на предпочитания по отношение на проследяването), неокончателна версия на автора, 7 март 2016 г.

<sup>16</sup> Работна група по член 29, WP 294, Становище 04/2012 относно освобождаването от изискването за съгласие за някои „бисквитки“, прието на 7 юни 2012 г., url: [http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2012/wp194\\_bg.pdf](http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2012/wp194_bg.pdf).

<sup>17</sup> Пак там.

това да бъде строго необходимо. Пропускането на думата „строго“ може да не е умишлено, тъй като в съображение 21 от предложения регламент действително се посочва, че не следва да се иска съгласие за вмешателство, когато то е „строго“ необходимо. Независимо от това предложеният регламент представлява възможност допълнително да се поясни, че проверката на необходимостта в контекста на този регламент следва да се тълкува в тесен смисъл по отношение на всички изключения. Поради това Работната група предлага по отношение на всички изключения в член 6 и член 8, параграф 1 от предложения регламент пред „необходимо“ да се добави думата „строго“.

От друга страна Регламентът за неприкосновеността на личния живот и електронните съобщения следва изрично да позволява вмешателство в устройствата с цел инсталиране на актуализации за сигурност. Изпращането на актуализации за сигурност през интернет е предпочитаният метод за инсталиране на такива актуализации на повечето устройства на крайни ползватели. Инсталирането на актуализации се счита за вмешателство в крайните устройства. Съществува легитимен интерес да се гарантира, че сигурността на тези устройства отговаря на последните развития. Поради това доставчикът на актуализации за сигурност като цяло следва да бъде в състояние да инсталира строго необходимите актуализации за сигурност без съгласието на крайния ползвател. Не е сигурно обаче дали това вмешателство може да бъде обхванато от изключението по отношение на „услуга на информационното общество“ от забраната за вмешателство (член 8, параграф 1, буква в). Следва да бъде пояснено, че инсталирането на актуализации за сигурност се позволява съгласно това изключение, но само при условие че i) актуализациите за сигурност са оформени като отделен пакет и по никакъв начин не променят функциите на софтуера на устройството (включително взаимодействието с друг софтуер или настройките, избрани от ползвателя), ii) крайният ползвател се информира предварително всеки път, когато се инсталира актуализация, и iii) крайният ползвател има възможност да изключи автоматичното инсталиране на тези актуализации.

## *ДИРЕКТЕН МАРКЕТИНГ*

Друга категория опасения е свързана с недостатъчната защита срещу директен маркетинг.

27. На първо място се пораждат опасения от факта, че **обхватът на определението за директен маркетинг е твърде ограничен**. В член 4, параграф 3, буква е) от предложения регламент „съобщение за целите на директния маркетинг“ е определено като „всяка форма на реклама, независимо дали е писмена или устна, изпратена от един или повече идентифицирани или идентифицируеми крайни ползватели на електронни съобщителни услуги“. Думата „изпратена“ предполага използването на технологични комуникационни средства, което по необходимост включва предаването на съобщение, докато по-голямата част от рекламирането в интернет (чрез платформите на социалните медии или в различни уебсайтове) не включва „изпращане“ на реклами в прекия смисъл.



Това се подчертава допълнително от примерите, които се посочват в това определение (SMS, електронна поща) и в съображение 33. Всички те са свързани с доста традиционни форми на маркетингови съобщения и дори използването на — също доста традиционни — повикващи системи определено не попада в рамките на обхвата. Посоченият член и съображението следва да бъдат изменени, така че да включват всички реклами, които са *изпратени, насочени или представени* на един или повече идентифицирани или идентифицируеми крайни ползватели. Освен това следва да се гарантира допълнително, че поведенческите реклами (въз основа на профилите на крайните ползватели) също се считат за съобщения за целите на директния маркетинг, насочени към „един или повече идентифицирани или идентифицируеми крайни ползватели“ (сами по себе си рекламира са насочени към конкретни, идентифицируеми ползватели).

В допълнение към това в съответствие с предложения обхват на „съобщенията на директния маркетинг“ защитата съгласно член 16, параграф 1 ще бъде ограничена до съобщения, които съдържат рекламни материали, и лицата няма да бъдат защитени от други съобщения, които са изпратени, насочени или представени с маркетингова цел (като например съобщения за искане на съгласие, свързани с генериране на лийдове, популяризиране на политически възгледи или предпочитания при гласуване, популяризиране на благотворителни или други организации с нестопанска цел или общо популяризиране на марката на дадена организация). Освен това факс машините все още се използват като средство за директен маркетинг, въпреки че не са посочени в определението. Поради това член 4, параграф 3, буква е) следва да включва всички форми на реклама, агитационна активност или популяризиране, включително за организации с нестопанска цел, и следва изрично да включва факс машини успоредно с електронна поща и SMS (вж. също така предложението за пояснение в точка 43, буква а). На последно място, в съображение 32 се посочва, че директният маркетинг включва съобщения, изпращани от политически партии, за да провеждат кампании за популяризиране. Този текст следва да се актуализира, така че да включва политици и кандидати за участие в избори, които популяризират своята кандидатура.

28. Второ, **оттеглянето на съгласието за директен маркетинг не е безплатно и не е толкова лесно, колкото даването на съгласие**. Възможността за оттегляне на съгласието в съответствие с предложения регламент трябва да бъде пояснена, за да се гарантира съгласуваност и да се подобри защитата на получателите на маркетингови съобщения. Понастоящем в член 16, параграф 6 от предложения регламент се предвижда, че на получателите на съобщения на директния маркетинг трябва да се предостави „необходимата информация, за да могат те да упражнят правото си да оттеглят по лесен начин своето съгласие за получаването на по-нататъшни маркетингови съобщения“ (подчертаването е добавено). Това е потвърдено в съображение 34. От съображение 70 от ОРЗД обаче следва, че субектите на данни съгласно ОРЗД следва не само да имат право да възразят срещу обработването за целите на директния маркетинг, но и да могат да го направят „безплатно“. Този израз се използва и в член 16,

параграф 2 от предложения регламент, но само във връзка с отказ от директен маркетинг въз основа на данни за контакт, получени в контекста на продажба.

В член 7, параграф 3 от ОРЗД се предвижда, че оттеглянето на съгласие е също толкова лесно, колкото и даването му, и че лицата следва да бъдат в състояние да оттеглят съгласието си по всяко време. Освен това в своето Становище 04/2010 относно FEDMA (WP174) Работната група вече отчете колко е важно на лицето да се предостави „лесен, ефективен, безплатен, пряк и леснодостъпен начин да се отпише“ от директния маркетинг<sup>18</sup>. Този стандарт за оттегляне на съгласието следва да бъде включен в правилата за директния маркетинг в предложения регламент. Същото важи за изискването в член 7, параграф 3 от ОРЗД, че оттеглянето на съгласие следва да бъде също толкова лесно, колкото и даването му, и то по всяко време.

29. В тази връзка следва да се поясни начинът за оттегляне на съгласието или за отказ от повиквания за целите на директния маркетинг. Въз основа на член 16, параграф 4 от предложения регламент държавите членки могат да изберат режим на отказ от гласови повиквания за маркетингови цели. В Регламента за неприкосновеността на личния живот и електронните съобщения следва да се посочат договореностите за оттегляне на съгласието и за отказ от повиквания за маркетингови цели. В съображение 36 се посочва, че държавите членки *следва да могат* да установят и/или поддържат национални системи за отказ от такива повиквания. Следователно въз основа на тази разпоредба държавите членки биха могли да позволят дори ситуация, в която ползвателят трябва да отказва на всеки отделен доставчик на съобщителни услуги. При такова прилагане ползвателите не са защитени от досадни нежелани съобщения<sup>19</sup> и не се осигурява отговарящ на ОРЗД механизъм, чрез който съгласието да се оттегля лесно и по всяко време. Поради това в Регламента следва да се посочва, че всяка държава членка *трябва* да създаде национален регистър за отказ от повиквания. Освен това в Регламента следва да се посочва, че на получателите на гласови повиквания следва да се осигурят два варианта за оттегляне на съгласието: за бъдещи повиквания от това дружество или организация и възможност за регистриране в национален регистър за отказ от повиквания по време на тези повиквания.

30. Друг повод за опасение е липсата на изрична забрана за използването на фалшива самоличност при изпращането на съобщенията на директния маркетинг. В съображение 34 се отбелязва, че е забранено „прикриването на самоличността и използването на фалшива самоличност и фалшиви адреси или номера за отговор при изпращането на нежелани търговски съобщения за

---

<sup>18</sup> Работна група по член 29, WP174, Становище 4/2010 относно Европейския кодекс за поведение на Европейската федерация за директен маркетинг (FEDMA) за използването на лични данни при директен маркетинг, прието на 13 юли 2010 г., url: [http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2010/wp174\\_bg.pdf](http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2010/wp174_bg.pdf)

<sup>19</sup> Например в Обединеното кралство операторът на далекосъобщителни услуги BT отчете 31 милиона досадни обаждания за една седмица. Вж.: <http://www.bbc.com/news/business-38635921>.

целите на директния маркетинг“. В член 16, параграф 6 обаче се посочва единствено, че крайните ползватели се информират за „самоличността на физическото или юридическото лице, от името на което се предава съобщението“. Това задължение за информиране на получателите относно самоличността следва да бъде допълнено от ясна забрана за използването на прикрити или фалшиви адреси за целите на директния маркетинг.

31. Този въпрос е свързан и с друг повод за опасение: **изискването за код за повиквания за целите на директния маркетинг е представено като алтернатива на изискването за представяне на идентификация на линия за осъществяване на връзка**. Съгласно член 16, параграф 3 повикванията за целите на директния маркетинг са позволени, ако обаждащият се може или i) да представи идентификация на линия, чрез която може да се осъществи връзка с физическото или юридическото лице, което извършва повикването (член 16, параграф 3, буква а), или ii) да използва специфичен код, който да идентифицира повикването като рекламно (член 16, параграф 3, буква б). Въпреки че Работната група приветства задължението в член 16, параграф 3, буква б) да се използва код, тя счита, че това изискване касае същия проблем, към който е насочено задължението за идентификация на линия в член 16, параграф 3, буква а). Докато целта на изискването за код е да се позволи на получателя да идентифицира веднага повикването като рекламно (и да предприеме мерки за блокирането на тези повиквания), целта на изискването за идентификация на линия е да се осигури средство за получателите (и надзорните органи), чрез което може да се идентифицира и осъществи връзка с инициатора на рекламното повикване. Това е от особено значение по отношение на автоматизираните повиквания, при които е налице сериозна неравнопоставеност между възможностите на търговеца да изпраща досадни обаждания и възможностите на получателя да ги избягва. Поради това изискванията не трябва да бъдат алтернативи, а да се допълват взаимно.

#### *ГРАФИК*

32. Работната група по член 29 приветства Европейската комисия за отчитането на необходимостта предложеният регламент да влезе в сила успоредно с ОРЗД през май 2018 г., за да се избегнат несъответствия между двата законодателни акта. При все това се поражда опасения от факта, че това е амбициозен график, който изисква и финализиране на проекта на ЕКЕС. Поради това РГ29 отправя искане към всички заинтересовани страни в законодателния процес да се ангажират с крайния срок през май 2018 г.

#### *ДРУГИ ОПАСЕНИЯ*

В настоящия раздел се обсъждат някои допълнителни опасения.

33. На първо място РГ29 изразява опасение относно **допускането, че нецеленасочените мерки за запазване на данни са приемливи**. В обяснителния меморандум се отбелязва, че съгласно предложения регламент

държавите членки са свободни да запазят или създадат национални рамки за запазването на данни, които, наред с другото, предвиждат целенасочени мерки за запазване (точка 1.3). След решението по делото *Tele2/Watson*<sup>20</sup> е ясно, че рамките за запазване на данни, които предвиждат нещо различно от целево запазване, не са разрешени съгласно Хартата (а дори и тогава биха подлежали на важни условия, например надзор) и че общият достъп до метаданни ще трябва да се разглежда като нарушение на същността на член 7 по същия начин като общия достъп до съдържанието на електронни съобщения (вж. решение на Съда на ЕС по делото *Schrems* и съображение 94). Поради това формулировката на това изречение изглежда оставя известна свобода на действие на държавите членки по отношение на мерки за запазване на данни, каквато всъщност не съществува. В тази връзка предложеният регламент **не осигурява достатъчно ниво на защита на метаданните**. Както е отбелязано в точка 10, Работната група по член 29 приветства признанието, че метаданните могат да разкрият много чувствителни данни. При все това предложеният регламент не осигурява на метаданните защитата, която би следвало да произтича от това признание. Предвид по-специално на чувствителността на данните, преди извършването на анализ по силата на член 6, параграф 2, буква в) следва да се извърши ОВЗД (вж. също така точка 46).

34. Второ, **предложеният регламент би довел до нежелателно разширяване на възможностите за запазване на данни**. В член 11 от предложения регламент се посочва член 23, параграф 1, букви а)—д) от ОРЗД при описанието на целите, за които държавите членки могат да ограничат задълженията и правата, предвидени в членове 5—8 от Регламента. В ОРЗД не се предвиждат такива ограничения по отношение на специални категории данни в съответствие с високите рискове за субектите на данни. Макар че в член 15 от Директивата за правото на неприкосновеност на личния живот и електронни комуникации понастоящем се предвижда подобно ограничение, неговите цели са по-ограничени. Предложеният регламент ще позволи нови ограничения за целите на „изпълнението на наложените наказания, включително предпазването от и предотвратяването на заплахи за обществената сигурност“ (член 23, параграф 1, буква г) от ОРЗД) и „други важни цели от широк обществен интерес за Съюза или за държава членка, и по-специално важен икономически или финансов интерес на Съюза или на държава членка, включително паричните, бюджетните и данъчните въпроси, общественото здраве и социалната сигурност“ (член 23, параграф 1, буква д) от ОРЗД). Тези цели не само са нови в сравнение с Директивата за правото на неприкосновеност на личния живот и електронни комуникации, но освен това последната цел на член 23, параграф 1, буква г) и цялостната цел на член 23, параграф 1, буква д) са формулирани твърде общо. Поради това се предлага да се заличат препратките към член 23, параграф 1, букви а)—д) от ОРЗД и вместо това да се посочат само целите, които понастоящем се съдържат в член 15 от Директивата за правото на неприкосновеност на личния живот и електронни комуникации.

<sup>20</sup> ECLI:EU:C:2016:970, url: <http://curia.europa.eu/juris/celex.jsf?celex=62015CJ0203>.

35. **Задължението за информиране на ползвателите относно рисковете за сигурността има минимален обхват.** Работната група приветства факта, че доставчиците на услуги трябва да информират ползвателите относно рисковете за сигурността и мерките за намаляване на тези рискове, например криптиране (член 17 и съображение 37). Заглавието на разпоредбата обаче гласи „Информация за установени рискове за сигурността“. Фактът, че в заглавието се говори за установени рискове, предполага, че тази разпоредба е свързана само с (потенциални) нарушения на сигурността, докато текстовете на разпоредбата и съображението са насочени по-скоро към общото информиране на крайните ползватели. Например, ако доставчик на услуги установи, че устройството на ползвателя е заразено със зловреден софтуер и е станало част от ботнет, тази разпоредба изглежда налага пряко задължение на доставчика да информира ползвателя относно произтичащите от това рискове. Обхватът на тази разпоредба обаче би могъл да се поясни и не следва да бъде ограничен до този конкретен сценарий. Разпоредбата следва да обхване най-малко установените рискове за сигурността във всички устройства, предоставени на крайния ползвател от доставчика като част от абонамента, като например рутери и мобилни устройства, и да включва информиране относно рисковете от промяна на настройките, които са насочени към защита на неприкосновеността на личния живот съгласно принципа на защита на данните на етапа на проектирането.

Работната група препоръчва обхватът да се разшири, така че да включва доставчици на софтуер, позволяващ електронни съобщения (вж. съображение 8), и също така евентуално нова категория: доставчици на технологии от съществено значение за сигурността на съобщенията, които не са доставчици на услуги (например доставчици на криптиращи технологии). Ако се добави последната категория, следва да се обърне внимание това задължение да не се припокрива със задълженията за уведомяване при нарушение на сигурността съгласно други инструменти, като например Директивата относно мрежите и информационните системи<sup>21</sup> и други правни инструменти, касаещи доставчиците на сертификати. Тъй като доставчиците от последната категория обикновено не осъществяват пряк контакт с крайните ползватели, трябва също така да се обясни по какъв начин те могат да спазят своето задължение за информиране съгласно тази разпоредба.

36. Работната група приветства разпоредбите в членове 2 и 13, които ще се прилагат към междуличностни съобщителни услуги посредством номер. При все това не е ясно **защо не следва да се осигури подобно ниво на защита на данните по отношение на функционално равностойните ОТТ услуги за повиквания.**

---

<sup>21</sup> Директива (ЕС) 2016/1148 на Европейския парламент и на Съвета от 6 юли 2016 г. относно мерки за високо общо ниво на сигурност на мрежите и информационните системи в Съюза, ОВ L 194, 19.7.2016 г., стр. 1—30, url: [http://eur-lex.europa.eu/legal-content/BG/TXT/?uri=uriserv%3A0J.L\\_2016.194.01.0001.01.ENG](http://eur-lex.europa.eu/legal-content/BG/TXT/?uri=uriserv%3A0J.L_2016.194.01.0001.01.ENG)

37. Работната група също така изразява загриженост относно **липсата на яснота във връзка с диференцираното съгласие за обратно търсене в указателите**. Съгласно член 15, параграф 2 от предложения регламент доставчиците са длъжни да получат съгласие от крайните ползватели, преди да разрешат използване на функциите за търсене във връзка с данни (вж. също така съображение 31). Работната група приветства хармонизирането на изискването за съгласие по отношение на включването в указатели, но изразява съжаление относно липсата на диференцираност по отношение на различните видове търсене. Директивата за правото на неприкосновеност на личния живот и електронни комуникации, която понастоящем е в сила, позволява на държавите членки да въведат изискване за отделно съгласие по отношение на обратното търсене въз основа на член 12, параграф 3. Този член гласи, че *„държавите членки могат да изискват за всяка цел на публичен указател, освен тази за търсене на координати на лица на база техните имена и когато е необходимо минимален брой други идентификатори, да бъде поискано допълнително съгласие от абонатите“*. Въз основа на тази разпоредба в редица държави членки се изисква отделно съгласие във връзка с функциите за обратно търсене, като се отчитат различните нива на възможностите за идентифициране и съответно вмешателството на двете функции в неприкосновеността на личния живот.
38. От по-формална гледна точка **нивото на глобите не е хармонизирано за всички нарушения на Регламента**. Съгласно предложия регламент държавите членки определят правилата относно глобите за нарушения на член 23, параграф 4, член 23, параграф 6 и член 24 от предложия регламент. Би било по-последователно, ако това бъде предвидено и в самия регламент за неприкосновеността на личния живот и електронните съобщения.
39. На последно място, в **предложия регламент се разчита на определения, които могат да се превърнат в „подвижни цели“**. По отношение на редица ключови понятия в предложия регламент се прави препратка към друг правен инструмент, който понастоящем се изготвя: предложият ЕКЕС (вж. например член 4, параграф 1, буква б). Два важни примера за това са определението на „краен ползвател“, което понастоящем включва физически и юридически лица, и определенията на „електронна съобщителна услуга“ и „междудличностна съобщителна услуга“, които са отразени в член 4, параграф 1, буква б) от предложия регламент, а по отношение на последната в член 4, параграф 2 се посочва по-подробно, че определението включва видове услуги, които изрично са изключени от ЕКЕС<sup>22</sup>. Настоящото становище е основано на определенията в сегашния им вид, но има голяма вероятност предложият ЕКЕС и/или

---

<sup>22</sup> Например в член 4, параграф 2 от предложия регламент се посочва, че междудличностната съобщителна услуга „включва услуги, които позволяват междудличностна и интерактивна комуникация само като незначителна допълнителна възможност, неразделно свързана с друга услуга“, докато в член 2, параграф 5 от ЕКЕС тези услуги специално се изключват от това определение. (ЕКЕС включва „междудличностната съобщителна услуга“ в рамките на по-широкообхватната категория „електронна съобщителна услуга“ в член 2, параграф 4).

основните му понятия да се променят. Това би имало непосредствени последици за Регламента за неприкосновеността на личния живот и електронните съобщения. В идеалния случай в Регламента за неприкосновеността на личния живот и електронните съобщения всички понятия, произтичащи от ЕКЕС, следва да бъдат самостоятелно определени, или като минимум предложеният регламент следва да включва пояснение, когато се използват понятия, чиито определения се различават от посочените в ЕКЕС (например горепосоченото включване на „спомогателни услуги“ в определението за „междупersonна съобщителна услуга“). Ако това обаче не е възможно, според Работната група всички страни, участващи в законодателния процес, следва да гарантират, че предложеният регламент и ЕКЕС се обсъждат и гласуват едновременно, за да могат заинтересованите страни правилно да оценят обхвата и отражението на новите инструменти.

## **5. ПРЕДЛОЖЕНИЯ ЗА ПОЯСНЕНИЯ С ЦЕЛ ОСИГУРЯВАНЕ НА ПРАВНА СИГУРНОСТ**

В допълнение към разгледаните по-горе точки Работната група също така желае да насочи вниманието към някои разпоредби от предложения регламент, които би било полезно да се пояснят. Тези пояснения се считат за необходими, за да се повиши правната сигурност на всички заинтересовани страни, че ще бъде налице единно разбиране и прилагане на Регламента за неприкосновеността на личния живот и електронните съобщения навсякъде в ЕС.

### *ПОЯСНЕНИЯ ОТНОСНО ОБХВАТА*

40. Що се отнася до обхвата на предложения регламент, РГ29 предлага следните пояснения:

- а. **Понятието „краен ползвател“ следва да включва всички индивидуални ползватели.** В член 2, параграф 14 от ЕКЕС „краен ползвател“ се определя като ползвател, който не предоставя обществени съобщителни мрежи или обществено достъпни електронни съобщителни услуги. Следва да се поясни, че лицата, които допринасят за мрежите — например за решетъчни мрежи чрез своя рутер с WiFi — не са изключени от обхвата на защитата съгласно предложения регламент.
- б. **Следва да се поясни, че в териториалния обхват попадат всички крайни ползватели в Съюза.** В член 3, параграф 1, буква а) се посочва, че предложеният регламент се прилага за предоставянето на електронни съобщителни услуги на крайните ползватели „в Съюза“, докато в член 3, параграф 1, буква в) се посочва, че той се прилага за защитата на крайните устройства на крайните ползватели, „намиращи се в Съюза“ (подчертаването е добавено). Тази формулировка се различава в отделните преводи. Преводът на немски език не съдържа такова разграничение, докато други, като например преводите на френски, испански и нидерландски език, го съдържат. От съображение 9 става ясно, че териториалният обхват е предвиден да бъде широк, без

значение дали услугите се предоставят от място извън Съюза или обработването се извършва в Съюза. Поради това се предлага изразът „намиращи се“ да отпадне от член 3, параграф 1, буква в), за да се подчертае този широк обхват.

**в. Предложеният регламент изглежда защитава единствено преминаването на поверителни данни, но не и съхранението им.**

Възприетият понастоящем подход в предложения регламент е вниманието да се насочи към защита при предаването на съобщения. Вж. например съображение 15, което гласи, че забраната за прихващане на данни от съобщения следва да се прилага по време на предаването им, т.е. до получаването на съдържанието на електронното съобщение от лицето, за което е предназначено. Обхватът на тази защита се основава на концептуална рамка за съобщения, която е остаряла. Повечето данни от съобщения продължават да се съхраняват от доставчиците на услуги дори след като съобщенията бъдат получени. Следва да се гарантира, че поверителността на тези данни продължава да бъде защитена. Освен това комуникацията между абонати на едни и същи услуги, основани на изчисления в облак (например доставчици на уеб-базирани пощи), често е свързана в много малка степен с предаване: изпращането на писмо е свързано най-вече с отразяването на това в базата данни на доставчика, а не с реално изпращане на съобщения между две страни. Аргументът, че този въпрос вече е обхванат от ОРЗД, не е убедителен: принципната идея на предложения регламент е да се защити всяка поверителна комуникация, независимо от техническите средства за осъществяването ѝ. Възможно е това да представлява просто грешка при съставянето на текста, тъй като забраната в член 5 е свързана със „съхранение“ и „обработване“.

**г. Всички горещи точки за публичен безжичен достъп до интернет следва да попадат в рамките на обхвата.** Тъй като използването на безжични горещи точки е обичайна практика, логично е да няма съмнение дали поверителността на съобщенията, предавани чрез тези горещи точки, е защитена. Опитът това да се поясни в Регламента обаче е неуспешен, тъй като в рамките на обхвата попадат само мрежи, предоставени на „неопределена група от крайни ползватели“ (съображение 13). Трябва да се въведат определения на изразите „неопределена група от крайни ползватели“ и „затворена група крайни ползватели“. По-специално следва да се поясни, че сигурните безжични мрежи (т.е. с парола) също попадат в рамките на обхвата, ако тази парола се предоставя на теоретично неопределена група от крайни ползватели, чиято самоличност не може да бъде определена предварително (например клиенти на кафене, посетители на летище). В съответствие с предходното становище на РГ29 относно прегледа на Директивата за правото на неприкосновеност на личния живот и електронни комуникации залегалят в основата принцип в този контекст е, че *„от инструмента за правото на неприкосновеност на личния живот и електронни комуникации могат да бъдат изключени само услуги, предоставяни в рамките на официални или трудови*



*взаимоотношения и свързани единствено със служебни или официални цели, или технически съобщения между публични или различни от публични органи единствено за контролиране на работни или бизнес процеси, както и използването на услуги изключително за лични цели“ (стр. 8).*

- д. **Данните, събрани по време на предоставянето на цифровите разпръсквателни услуги, следва да бъдат обхванати от предложения регламент.** Предвид чувствителното естество на поведението, свързано с гледане на предавания, тъй като то разкрива личните интереси и характеристики на зрителите, в Регламента за неприкосновеността на личния живот и електронните съобщения следва да се посочи (може би посредством съображение), че изключването на услуги за осигуряване на „съдържание, предавано посредством електронни съобщителни мрежи“ от определението на „електронна съобщителна услуга“ (ЕСУ) не означава, че доставчиците на услуги, които предлагат както ЕСУ, така и услуги за съдържание, не попадат в обхвата на разпоредбите на Регламента за неприкосновеността на личния живот и електронните съобщения, който е насочен към доставчиците на ЕСУ. Това е от особено значение, тъй като предоставянето на услуги за осигуряване на „съдържание, предавано посредством електронни съобщителни мрежи“ е изключено от определението на „електронна съобщителна услуга“ в предложения ЕКЕС (член 2, параграф 4).
- е. **Данните от съобщения като цяло представляват лични данни.** В съображение 4 се отбелязва, че данните от съобщения може да включват лични данни. При все това повечето данни от съобщения представляват лични данни<sup>23</sup> и в по-голямата си част това са данни от доста лично и чувствително естество, поради което изречението следва да се измени и да гласи, че тези данни като цяло представляват лични данни.
- ж. **Поверителната комуникация включва съобщенията, обменяни в рамките на дадена платформа.** В съображение 1 се обяснява, че принципът на поверителност се прилага по отношение на „съществуващи и бъдещи средства за комуникация“. След това в съображението се изброяват примери за такива средства, включително „лични съобщения, осигурявани от социалните медии“. Целта вероятно е да се включат личните съобщения между ползвателите на социална мрежа (например Facebook или Twitter) или съобщения, публикувани на стената на даден ползвател, които са достъпни за ограничен брой лица, но формулировката на текста не е достатъчно ясна.
- з. **Начин, по който Регламентът за неприкосновеността на личния живот и електронните съобщения се прилага към предаването на съобщения между машини.** Както е посочено в точка 9, Работната

---

<sup>23</sup> Вж. например решение на Съда на ЕС от 6 ноември 2003 г., C-101/01, точка 24 (по отношение на телефонен номер), решение на Съда на ЕС от 19 октомври 2016 г., C-582/14 (*Breyer*), точка 49 (по отношение на динамични IP адреси) и решение на Съда на ЕС от 8 април 2014 г., C-239/12 и C-594/12 (*Digital Rights Ireland*), точки 26—27 (по отношение на чувствителността на метаданните).

група приветства разширяването на защитата, така че да се обхване и предаването на съобщения между машини. Това обаче е посочено само в съображение 12, но не и в съответстващ член. Тази защита е желателна, тъй като тези съобщения често съдържат информация, която е защитена съгласно правото на неприкосновеност на личния живот. От друга страна следва да се въведе изключение за ограничена категория съобщения, които се предават изцяло между машини, ако те не оказват въздействие върху неприкосновеността или поверителността на съобщенията, какъвто е случаят например, когато комуникацията се извършва във връзка с изпълнението на протоколи за предаване между мрежовите елементи (например сървъри, комутатори), за да се известяват един друг, че са активни.

Един конкретен контекст, в рамките на който прилагането на Регламента за неприкосновеността на личния живот и електронните съобщения изисква пояснение, е областта на интелигентните транспортни системи. Предвижда се превозните средства постоянно да предават данни посредством радиовълни данни, съдържащи уникален идентификатор. Без допълнителната защита, предвидена в Регламента за неприкосновеността на личния живот и електронните съобщения, това би могло да доведе до непрекъснато следене на начина на кормуване, маршрутите и скоростта на водачите. Член 2, параграф 1 от ЕКЕС обаче съдържа ново и разширено определение на съобщителните мрежи. Те включват преносни системи, които не разполагат с централизиран административен капацитет и не позволяват пренос на сигнали посредством радиовълни. В съображение 14 от Регламента за неприкосновеността на личния живот и електронните съобщения се посочва, че тези данни представляват данни от електронни съобщения. Въз основа на член 5 от предложения регламент се забранява всеки вид прихващане, наблюдение или съхранение на тези данни от електронни съобщения, освен когато се прилага някое от изключенията. Въпреки това е налице интерес за обработването на тези данни, които позволяват на обекти като автоматично управлявани автомобили и устройства да се предупреждават взаимно относно обкръжението им или други рискове. Следователно въпросът е какво изключение да се прилага в този случай. Изключението въз основа на съгласието от крайните ползватели не е осъществимо, защото може да възникне необходимост тези данни винаги да могат да се обработват. Поради това доставчиците следва да бъдат в състояние да използват специално изключение, което позволява на обекти като автоматично управлявани автомобили и устройства да се предупреждават взаимно относно обкръжението им или други рискове.

#### *ПОЯСНЕНИЯ ОТНОСНО ПОНЯТИЕТО ЗА СЪГЛАСИЕ И ПРИЛАГАНЕТО МУ*

41. Що се отнася до понятието за съгласие и прилагането му в предложения регламент в сегашния му вид, РГ29 предлага следните пояснения:

- а. **Начин, по който понятието за съгласие следва да се прилага в контекста на юридическите лица.** В съображение 3 се отбелязва, че регламентът следва да гарантира, че разпоредбите на ОРЗД се прилагат и спрямо крайни ползватели, които са юридически лица. Съгласно съображението това включва и определението на понятието „съгласие“ в съответствие с ОРЗД (вж. също така съображение 18). Както е отбелязано в точка 13, Работната група приветства изричното включване на юридическите лица в обхвата на Регламента. Практическото прилагане на този принцип обаче не е ясно. Съгласно определението на понятието „съгласие“ в съответствие с ОРЗД се изисква то да бъде „информирано“, а указанието за волята на субекта на данните трябва да бъде „посредством изявление или ясно потвърждаващо действие“ (член 4, параграф 11 от ОРЗД). Трябва да се поясни в кои случаи юридическото лице реално може да се счита за „информирано“ и кога е налице такова изразяване на волята на юридическото лице.
- б. В този контекст следва да се отбележи, че при повечето обстоятелства работодателят може да не изразява съгласие от името на своите служите, защото когато работодателят се нуждае от съгласието на даден служител и с оглед на неравнопоставеността на силите възниква действителна или потенциална промяна в нагласата спрямо служителя, произтичаща от несъгласието на служителя, съгласието не е валидно, тъй като не е свободно изразено<sup>24</sup>. Що се отнася до **дружествата, които предоставят устройства или оборудване на физически лица, предложеният регламент не съдържа (подходящо) изключение** от забраната за вмешателство. Като пример може да се посочи случаят, когато работодателят желае да извърши актуализация на предоставен от дружеството телефон. Като друг пример работодателят предлага на служителите автомобили на лизинг и за административни цели позволява на трета страна да събира данни за местонахождението чрез бордово устройство, поставено в автомобила. И в двата случая служителят има интерес да осъществява вмешателство в тези устройства.
- Това вмешателство не може да се счита за необходимо за предоставянето на услуга на информационното общество (член 8, параграф 1, буква в) или необходимо за измерване на интернет аудиторията (член 8, параграф 1, буква г). Този проблем може да бъде решен чрез създаването на ново изключение, което включва ситуации, в които i) работодателят предоставя определено оборудване в контекста на трудово или служебно правоотношение, ii) служителят е ползвател на това оборудване и iii) вмешателството е строго необходимо за използването на оборудването от служителя (което предполага

---

<sup>24</sup> Вж. Становище 15/2011 относно понятието „съгласие“ (WP 187), Становище 8/2001 относно обработването на лични данни в контекста на трудово или служебно правоотношение (WP48) и новото становище относно обработването на данни на работното място (прието едновременно с настоящото становище).

прилагането на принципите на пропорционалност и субсидиарност по отношение на събирането на данни). За работодателя следва да бъде възможно да осъществи вмешателство в устройството на крайния ползвател само ако са изпълнени тези условия.

- в. **Подобряване на контрола с цел спиране на автоматичното препращане на повиквания.** В член 14 се предвижда важно средство за контрол за крайните ползватели с цел спиране на автоматичното препращане на повикването от трета страна. Тази защита може да бъде подобрена допълнително чрез изискване на съгласието на крайния ползвател, за да може изобщо да се пристъпи към препращане на повикването.

#### *ПОЯСНЕНИЯ ОТНОСНО МЕСТОНАХОЖДЕНИЕТО И ДРУГИ МЕТАДАННИ*

42. Работната група предлага да се поясни следното по отношение на местонахождението и други метаданни:

- а. Значението на израза **„данните за местоположението, генерирани извън контекста на предоставянето на електронни съобщителни услуги“** в съображение 17 следва да се поясни. Не е ясно дали той е свързан с данните за местонахождението, които се събират например чрез приложения, използващи данни от GPS функцията на интелигентни устройства, и/или с генериране на данни за местонахождението въз основа на разположени наблизо WiFi рутери и/или данни за местонахождението, събрани чрез бордови асистент навигатор, и/или други начини за генериране на данни за местонахождението. Тази липса на яснота поражда правна несигурност по отношение на обхвата на задължението. Във всеки случай данните за местонахождението на крайното устройство на физическо лице представляват лични данни и следователно обработването на тези данни е обхванато от задълженията, произтичащи от ОРЗД.
- б. Следва да се поясни, че **по-голямата част от законосъобразното обработване на данните за местонахождението и други метаданни не изисква уникален идентификатор**. В съображение 17 се посочват т.нар. „топлинни карти“ като пример за търговско използване на метаданни на електронни съобщения от доставчиците на електронни съобщителни услуги. За създаването на обикновена топлинна карта обаче не са необходими уникални идентификатори, а е достатъчно просто статистическо преброяване. Друг пример, посочен в съображението — използването и натиска върху наличната инфраструктура — също може да се обхване от преброяване от определени измервателни точки, например чрез изготвяне на агрегирани статистически данни относно използването на пунктове за наблюдение на трафика, за да се осигурят данни за натиска на определено място в конкретен момент, без да е необходимо да се узнава и самоличността на засегнатите лица.

Освен това в съображението се посочва като пример изобразяването на движенията в определени посоки за определен период от време, при което е необходим уникален идентификатор за свързване на позициите на лицата през определени интервали. С този пример съображението изглежда легитимира допълнителното обработване на тези данни в подкрепа на анализа на големи информационни масиви. Единственото условие съгласно предложения регламент за този вид обработване на данни е задължението да се извърши оценка на въздействието върху защитата на данните, ако обработването *има вероятност да доведе до висок риск за правата и свободите на физическите лица*. Това условие не е достатъчно. Освен това то противоречи на задължението в член 6, че този вид обработване може да се извършва само със съгласието на ползвателите и само ако данните не могат да бъдат анонимизирани, т.е. без никакви уникални идентификатори. Ползвателите често не могат да откажат събирането на данните за тяхното географско местоположение от страна на доставчиците на електронни съобщителни услуги, когато това събиране технически е необходимо за предаването на съобщението до ползвателя или когато това обработване е необходимо за предоставяне на поисканата услуга (например навигация). В предишни становища Работната група заключи, че тези данни за местонахождението от интелигентни устройства представляват лични данни от чувствително естество и че ползите от анализа на тези данни нямат предимство пред правата на ползвателите във връзка със защитата на поверителността на метаданните на техните съобщения, нито имат предимство пред другите им общи права на защита на данните съгласно ОРЗД. Поради това в съображението трябва най-малкото да се посочва, че доставчиците трябва да спазват задълженията съгласно член 25 от ОРЗД в случай на по-нататъшно обработване на данните за местонахождението или други метаданни. Това означава, че трябва да бъдат предприети най-малкото следните мерки:

- i) използване на временни псевдоними;
- ii) заличаване на всички справочни таблици между тези псевдоними и първоначалните данни, които позволяват идентифициране;
- iii) агрегиране до равнище, на което отделните ползватели вече не могат да бъдат идентифицирани чрез конкретните им маршрути; както и
- iv) заличаване на стойностите, които значително се различават от нормалните и чрез които все още е възможно идентифициране (всички тези мерки трябва да се прилагат заедно).

На последно място, Регламентът за неприкосновеността на личния живот и електронните съобщения трябва да задължи страните, които участват в обработването на данните за местонахождението и други метаданни, да оповестят публично своите методи за анонимизиране и допълнително агрегиране, без да се засяга защитената по закон поверителност. Така ще се позволи на надзорните органи и на широката общественост лесно да проверят дали избраният метод е подходящ.

43. Работната група предлага да се поясни следното по отношение на нежеланите съобщения:

- а. **Формулировката на забраната за директен маркетинг, когато не е дадено съгласие.** В член 16, параграф 1 от предложения регламент понастоящем се отбелязва, че електронните съобщителни услуги „могат“ да се използват за целите на изпращане на съобщения на директния маркетинг (при наличие на съгласие), но не се посочва изрична забрана за изпращане (насочване или представяне) на съобщения на директния маркетинг, когато не е дадено съгласие. Това противоречи на подхода, възприет в други разпоредби, съгласно който първо се формулира забрана, която се следва от определени конкретни изключения. Настоящият текст предполага по-снизходителен подход (като целта вероятно не е била такава). Работната група предлага леко променен вариант на текста на настоящия член 13, параграф 1 от Директивата за правото на неприкосновеност на личния живот и електронни комуникации: Използването от физически или юридически лица на електронни съобщителни услуги, включително на гласови повиквания, автоматизирани повикващи системи и системи за комуникация, включително полуавтоматизирани системи, които свързват повиканото лице с физическо лице, машини за факсимилета, електронна поща или друг вид използване на електронни съобщителни услуги с цел представяне на съобщения на директния маркетинг на крайни ползватели, може да бъде позволено само по отношение на крайни ползватели, които са дали предварително своето съгласие.
- б. **Обхват на разпоредбите относно маркетинговите съобщения и повиквания към настоящи клиенти.** В член 16, параграф 2 се предвижда, че когато дадено лице получи данни за контакт за електронна поща от свой клиент, то може да използва тези електронни данни за контакт за допълнителен директен маркетинг на неговите собствени продукти или услуги, ако в момента на събирането на данни и всеки път, когато се изпраща съобщение, е дадена възможност да се възрази ясно, безплатно и по лесен начин. Понастоящем това е ограничено до данни за контакти с търговска цел, получени „в контекста на продажбата на продукт или услуга“ и за допълнителен маркетинг с търговска цел на собствени подобни продукти или услуги. Предвид факта, че разпоредбите за директния маркетинг се прилагат по същия начин към дейности за популяризиране с нетърговска цел (например на благотворителни организации или политически партии), тази разпоредба следва да се измени, така че да се прилага по същия начин към нетърговски организации, които се свързват с предишни поддръжници, когато популяризират свои подобни цели или идеали, и същото право на възражение следва да се прилага и при повиквания за целите на директния маркетинг. Освен това следва да бъде определен срок за валидността на данните за контакт на „настоящи клиенти“ в електронните съобщения с търговска, благотворителна или политическа

цел, като този срок следва да се прилага и при повиквания за целите на директния маркетинг. Когато държавите членки са избрали система за възразение срещу гласови повиквания за маркетингови цели, наличието на отношения на „настоящ клиент“ има предимство пред включването в регистър за отказ от повиквания. При тези обстоятелства крайните ползватели не разполагат с ефективна възможност да избегнат досадни обаждания от дружества или организации, с които веднъж са осъществили контакт и с които не желаят да контактуват повече. Поради това като основно правило в Регламента следва да се посочи валидността на това изключение за „настоящ клиент“, например една или две години, във връзка с основателните очаквания на съответните крайни ползватели.

- в. **Прилагане на правилата за директния маркетинг към юридически лица.** В член 16, параграф 5 от предложения регламент се предвижда, че държавите членки гарантират, че законните интереси на крайни ползватели, които са юридически лица, са достатъчно защитени по отношение на нежелани съобщения. В член 13, параграф 5 от настоящата Директива за правото на неприкосновеност на личния живот и електронни комуникации се описват законните интереси на абонати, различни от физически лица. Не е ясно какви ще бъдат последиците от тази промяна в текста. В съображенията следва да се поясни, че тази промяна не включва намерение за понижаване на нивото на защита. В тази връзка забраната за директен маркетинг, когато не е дадено съгласие, е насочена към „крайните ползватели, които са физически лица, дали съгласието си за това“ (подчертаването е добавено). Следва да се поясни, че това включва физически лица, *които работят за* юридически лица. От друга страна, не следва да се изисква съгласие за осъществяване на контакт с юридически лица чрез общи данни за контакти, които те са оповестили публично за тази цел (като например „info@companyname.eu“).
- г. **Прилагане на правилата за директен маркетинг към лица, които действат като (политически) представители:** В сегашния си вид член 16 може да възпрепятства изпращането на някои съобщения на избрани представители, в които се описват търговски съображения или интереси. Следва да се поясни, че регламентът не възпрепятства такива съобщения.

#### ПОЯСНЕНИЯ ОТНОСНО ПРИЛАГАНЕТО НА ИНСТРУМЕНТИ ЗА ОСНОВНИТЕ ПРАВА

44. Следва да се поясни допълнително **прилагането на Хартата и на Европейска конвенция за правата на човека (ЕКПЧ) към националните закони за запазване на данни.** В съображение 26 се предвижда, че всички мерки на държавите членки за защита на обществените интереси, като например мерки за законно прихващане, трябва да в съответствие с Хартата (в допълнение към ЕКПЧ). Това е желателно, тъй като в съответствие с обосновката в решението *Tele2/Watson* всички национални изключения от съдържащите се в правото на

ЕС предпазни мерки за защита при обработване на данните са обхванати от Хартата (и поради това нарушенията посредством неспазване на националните закони могат да бъдат отнесени пред Съда на Европейския съюз). В член 11 от предложениия регламент обаче се посочва само, че ограниченията на обхвата на членове 5—8 от предложениия регламент трябва да спазват по същество основните права и свободи и да представляват необходима и пропорционална мярка. В този член следва да се включи и изрична препратка към Хартата и ЕКПЧ.

**45. Поверителността на съобщенията е защитена и съгласно член 8 от ЕКПЧ.**

В точка 1.1 от меморандума и в съображение 1 се обяснява, че с предложениия регламент се изпълнява член 7 от Хартата. Това е повторено в съображение 19. Основното право на поверителност на съобщенията обаче не се защитава само с тази разпоредба, а и по силата на член 8 от ЕКПЧ. Добавянето на изрична препратка в член от предложениия регламент допълнително ще покаже, че всяка съответна съдебна практика на Европейския съд по правата на човека също трябва да се вземе предвид при оценката на (окончателния) регламент. Между другото, такава препратка вече е включена в съображения 20 (по отношение на крайните устройства) и 26 (по отношение на законното прихващане) и се подкрепя допълнително от съображенията в точка 2.1 от меморандума (относно връзката между Хартата и ЕКПЧ в контекста на юридическите лица), но не и в съответните членове, като например член 11, параграф 1.

*ДРУГИ ПОЯСНЕНИЯ*

**46. Следва да се поясни, че продължават да се прилагат задълженията съгласно ОРЗД, например по отношение на режима при нарушаване на сигурността на данните и по отношение на ОВЗД, когато страните обработват лични данни в контекста на данните от електронни съобщения. Както е посочено в съображение 5, че предложениият регламент е *lex specialis* по отношение на ОРЗД и че обработването на данните от електронни съобщения следва да се допуска само в съответствие с предложениия регламент, може да се повдигне въпросът дали определени задължения съгласно ОРЗД ще се прилагат и в контекста на предложениия регламент. Това е особено вярно в случаите, когато предложениият регламент би могъл да се тълкува в смисъл, че съдържа разпоредби за определено задължение, обхванато и от ОРЗД. Показателните примери включват:**

- i) предложениият регламент съдържа задължение за определено уведомяване за „установени“ рискове за сигурността (член 17) (вж. също така точка 35), докато ОРЗД съдържа режим за уведомление при нарушаването на сигурността на данните (членове 33 и 34);
- ii) в предложениия регламент се посочва, че извършването на ОВЗД и на консултация с надзорния орган в съответствие с ОРЗД е задължително при определени обстоятелства (съображения 17 и 19, както и член 6, параграф 3, буква б), докато в ОРЗД вече са определени случаите, при които трябва да се извърши ОВЗД, и случаите, в които се изисква консултация (членове 35 и 36); както и



- iii) не е посочено ясно, че ако дадено лице изпълни необходимите условия за изключение от забраната за обработване съгласно член 5 от предложения регламент, то пак ще трябва да спазва всички съответни задължения съгласно ОРЗД, когато става въпрос за обработване на лични данни, а всяко друго обработване на данни съгласно ОРЗД е забранено. Следва да се поясни, че поради това не се прилага проверката на съвместимостта, посочена в член 6, параграф 4 от ОРЗД.
- iv) В предложения регламент за неприкосновеността на личния живот и електронните съобщения не се предвиждат механизми за сертифициране, подобни на посочените в членове 42 и 43 от ОРЗД. Тъй като строго погледнато обхватът на член 42 от ОРЗД е ограничен до създаването на механизми за сертифициране за защита на данните и на печати и маркировки за защита на данните с цел да се демонстрира спазването на ОРЗД, следва да се обмисли дали не би трябвало да се въведе съпоставима разпоредба, която да позволи сертифициране на това, че операции по обработване, стандарти, продукти или услуги са в съответствие с Регламента за неприкосновеността на личния живот и електронните съобщения.

За да се гарантира, че тази липса на яснота не се използва като аргумент за понижаване на нивото на защита съгласно предложия регламент, следва да се посочи ясно, че във всички тези случаи администраторите трябва да спазват и ОРЗД.

47. Освен това следва да се поясни, че **изискването за оттегляне на съгласието се прилага и в контекста на вмешателство в крайното устройство**. В член 8, параграф 1, буква б) от предложия регламент се предвижда възможност за вмешателство в крайните устройства на крайните ползватели, ако те дадат своето съгласие. Съгласно член 9, параграф 3 се изисква крайните ползватели да получат възможността да оттеглят съгласието си по всяко време, но тази разпоредба се прилага само към съгласието за анализа на метаданни и съдържание. Следва да се поясни, че това задължение обхваща и вмешателството в крайните устройства.

48. В тази връзка следва да се поясни, че **напомнянето за възможността за оттегляне на съгласието се прилага и към съгласие, дадено чрез настройките на браузъра**. Съгласно член 9, параграф 3 се изисква на крайните ползватели да им бъде напомняно през периодични интервали от 6 месеца за възможността да оттеглят съгласието си по всяко време. Макар че Работната група счита, че общите настройки на браузърите и друг софтуер, включително на операционни системи, приложения и софтуерни интерфейси за устройства, свързани към т. нар. „интернет на предметите“ (т.е. които не са основани на специфичен диференциран контрол), не могат да представляват валидна мярка за даване на съгласие, тъй като общите настройки не са подходящи за даване на конкретно съгласие във връзка с конкретни сценарии (вж. точка 24), а настройките по подразбиране следва да бъдат лесни за използване (вж. точка 19). Ако това се запази в предложия регламент, настройките трябва да бъдат достатъчно диференцирани, за да се контролира цялото обработване на данни, за което ползвателят е дал своето съгласие, и да се обхванат всички функции на

устройството, които могат да доведат до обработване на данни. Освен това на крайния ползвател следва да бъде напомняно най-малкото през периодични интервали (от 6 месеца) за възможността да променя тези настройки.

49. Приветства се фактът, че съгласно предложения регламент се изисква софтуерът, който вече се предлага на пазара, да информира крайния ползвател относно вариантите за настройките за неприкосновеност (член 10). **При все това не е ясно по какъв начин тази разпоредба може да се приложи ефективно към по-стари продукти** и други продукти, които вече не се поддържат. Освен това следва да се предвиди допълнително пояснение по какъв начин това задължение ще се прилага към софтуер с отворен код, който се разработва по отворен и децентрализиран начин.
50. Следва да се поясни, че **предлагането на възможността за блокиране на „бисквитки“ (на трети страни) съгласно член 10 от предложения регламент има предимство пред изключението за измерване на интернет аудиторията** съгласно член 8, параграф 1, буква г). Или с други думи: макар че уебсайтът може да използва аналитични инструменти за измерване на интернет аудиторията съгласно член 8, параграф 1, буква г), ползвателите отново следва да имат право да блокират тези технологии за проследяване в своя браузър.
51. **Определението за (полу)автоматизирани повикващи системи и системи за комуникация следва да се поясни.** Определението на този израз в член 4, параграф 3, буква з) от предложения регламент съдържа препратка към самия израз във втората част от изречението („включително повиквания чрез използването на автоматизирани повикващи системи и системи за комуникация, които свързват повиканото лице с физическо лице“). Предлага се последното изречение да се заличи от определението и определението в член 4, параграф 3, буква ж) да се промени, така че да включва обаждания, извършени с помощта на полуавтоматизирани системи за комуникация, като например автоматизирани устройства за набиране на телефонни номера, които свързват повиканото лице с физическо лице
52. Следва да се поясни **информацията, която е „част от абонамента за услугата“.** В съображение 14 се посочва, че метаданните на електронните съобщения „може да включват информация, която е част от абонамента за услугата, когато такава информация се обработва за целите на предаването, разпространението или обмена на съдържание на електронни съобщения“. Не е ясно какво се цели с този текст.
53. Следва да се поясни **приложимостта на механизмите за съгласуваност и сътрудничество.** В съображение 38 се отбелязва, че при предложия регламент се разчита на механизма за съгласуваност на ОРЗД. Освен това в член 18, параграф 1 се предвижда, че глави VI и VII от ОРЗД се прилагат *mutatis mutandis*. В допълнение към това в член 19 се отбелязва, че Европейският комитет по защита на данните (ЕКЗД) изпълнява задачите, определени в член 70 от ОРЗД. Въпреки че прилагането на тези разпоредби е сравнително ясно, не може да се изключи възможността да възникнат въпроси

по отношение на тълкуването на основните понятия, свързани с механизмите за съгласуваност и сътрудничество съгласно ОРЗД. Например механизмът за водещ орган се прилага в случаите, когато е налице „трансгранично обработване“ (член 56, параграф 1 от ОРЗД): не е ясно как се прилага това в случай на вмешателство в крайното устройство или анализ на съдържанието или метаданните съгласно предложения регламент. Поради това е препоръчително да се поясни прилагането на тези основни понятия в съображение и да се подчертае, че всички нерешени въпроси относно приложимостта на тези глави от ОРЗД в контекста на предложения регламент ще бъдат решени чрез тълкуване на разпоредбите в тези глави в съответствие със заложената в тях цел. Освен това е препоръчително да се поясни, че член 70 се прилага *mutatis mutandis* към ЕКЗД в контекста на предложия регламент (понастоящем това липсва в съображението).

\* \* \*