



17/HU

WP 247

**01/2017. számú vélemény
az elektronikus hírközlési adatvédelmi rendeletről (2002/58/EK)**

Elfogadás időpontja: 2017. április 4.

Ez a munkacsoport a 95/46/EK irányelv 29. cikke alapján jött létre. A munkacsoport adatvédelemmel, valamint a magánélet védelmével kapcsolatos kérdésekkel foglalkozó független európai tanácsadó szerv. Feladatait a 95/46/EK irányelv 30. cikke és a 2002/58/EK irányelv 15. cikke határozza meg.

A titkársági feladatokat ellátja: Európai Bizottság, Jogértvényesülési és Fogyasztópolitikai Főigazgatóság, C Igazgatóság (Alapvető jogok és jogállamiság), B-1049 Brüsszel, Belgium, MO-59 05/035. sz. iroda.

Honlap: http://ec.europa.eu/justice/data-protection/index_en.htm

**AZ EGYÉNEKNEK A SZEMÉLYES ADATOK KEZELÉSE TEKINTETÉBEN VALÓ VÉDELMEVEL
FOGLALKOZÓ MUNKACSOPORT**

amelyet az 1995. október 24-i 95/46/EK európai parlamenti és tanácsi irányelvvel hoztak létre,

tekintettel az említett irányelv 29. és 30. cikkére,

tekintettel eljárási szabályzatára,

ELFOGADTA EZT A VÉLEMÉNYT:

ÖSSZEFOGLALÁS

A munkacsoport üdvözli az Európai Bizottság 2017. január 10-i, az elektronikus hírközlési adatvédelmi rendeletről szóló javaslatát. A munkacsoport üdvözli, hogy a szabályozási aktus a **rendelet formáját ölti**. Ez biztosítja, hogy a szabályok az Unió teljes területén egységesek legyenek, és biztosítja az áttekinthetőséget a felügyeleti hatóságok és a szervezetek számára. Emellett segíti az általános adatvédelmi rendelettel való összhang biztosítását is. Az összhangot segíti továbbá az a döntés is, hogy az elektronikus hírközlési adatvédelmi rendelet szabályainak érvényesítéséért **ugyanaz a hatóság feleljen, amely az általános adatvédelmi rendelet betartásának felügyeletéért felelős**.

Emellett a **kiegészítő jogi aktus** alkalmazása (fenntartása) is pozitívum. A bizalmas közlés és a végberendezések védelmének olyan sajátosságai vannak, amelyekre az általános adatvédelmi rendelet nem tér ki. Az ilyen szolgáltatásokra vonatkozó kiegészítő rendelkezésekre ezért szükség van a közlések titkossága és a magánélet tiszteletben tartásához való alapvető jog megfelelő védelméhez, beleértve a végberendezések titkosságát. E tekintetben a munkacsoport határozottan támogatja a javasolt rendeletben választott, **széles körű tilalmakra és szűk kivételekre épülő elvi megközelítést**, valamint a **hozzájárulás elvének célzott alkalmazását**.

A munkacsoport üdvözli a javasolt rendelet hatályának **kiterjesztését a hálózatsemleges online szolgáltatókra**, mint olyan szolgáltatásokra, amelyek működésük tekintetében a hagyományosabb hírközlési eszközökkel egyenértékűek, és ezért hasonló hatással lehetnek az unióban élők magánéletére és a közlések titkosságához való jogára. Pozitívum továbbá, hogy a javasolt rendelet egyértelműen kiterjed a **tartalmakra és a kapcsolódó metaadatokra**, elismerve, hogy a **metaadatok nagyon érzékeny adatokat fedhetnek fel**.

A munkacsoportban azonban négy **súlyos aggály** is felmerült. A **végberendezések helyének nyomon követése; a tartalom és a metaadatok elemzésének feltételei; a végberendezések és szoftverek alapbeállításai; valamint a hozzáférés feltételül szabott nyomonkövetési beleegyezés** terén a javasolt rendelet az általános adatvédelmi rendeletben biztosítotthoz képest csökkentené a védelem szintjét. A munkacsoport ebben a véleményben konkrét javaslatokat tesz annak biztosítására, hogy az elektronikus hírközlési adatvédelmi rendelet a kommunikációs adatok (mind a tartalom, mind a metaadatok) érzékeny jellegének megfelelő, ugyanolyan vagy magasabb szintű védelmet garantáljon.

Ami a **wifi alapú nyomon követést** illeti, a körülményektől és az adatgyűjtés céljától függően ilyen adatgyűjtés az általános adatvédelmi rendelet szerint várhatóan csak hozzájárulás birtokában, vagy csak abban az esetben folytatható, ha a gyűjtött személyes adatokat anonimizálják. Az utóbbi esetben a következő 4 feltételnek kell teljesülnie: a végberendezésről történő adatgyűjtés célja pusztán statisztikai számlálásra korlátozódik, a nyomon követés időben és térben az ehhez feltétlenül szükséges mértékre szorítkozik, az adatokat közvetlenül utána törlik vagy anonimizálják, és tényleges kívülmaradási lehetőségeket biztosítanak. Felkérjük az Európai Bizottságot, hogy ösztönözze egy olyan technikai standard létrehozását a mobil eszközök számára, amely automatikusan jelzi az ilyen nyomonkövetéssel szembeni kifogást.

A **tartalom- és metaadat-elemzés** terén a kiindulási pontnak annak kell lennie, hogy kommunikációs adatokat tilos feldolgozni, amíg ahhoz valamennyi végfelhasználó hozzá nem járult (küldők és címzettek egyaránt). Annak érdekében, hogy a szolgáltatók képesek legyenek a felhasználó által kifejezetten kért szolgáltatásokat, például keresési és indexálási funkciókat, vagy írott szöveg beszéddé alakítását nyújtani, az országok szintjén lehetővé kell tenni a kivételt a tartalom és metaadatok kizárólag a felhasználó személyes céljára történő kezelése tekintetében.

Ami a **nyomon követésbe való beleegyezést illeti**, a munkacsoport a hozzáférés feltételül szabott hozzájárulás, azaz az olyan megoldások kifejezett tiltására szólít fel, amelyek a felhasználót arra kényszerítik, hogy beleegyezzen a nyomon követésbe, ha hozzá kíván férni az adott szolgáltatáshoz.

Utoljára, de nem utolsó sorban a munkacsoport azt javasolja, hogy a végberendezések és a szoftverek **alapértelmezettként a magánélet védelmét biztosító beállításokat nyújtsanak**, és egyértelmű opciókat biztosítsanak a felhasználó számára ezeknek az alapértelmezett beállításoknak a megerősítése, illetve módosítása tekintetében az üzembe helyezés során. Ezeknek a beállításoknak az üzemeltetés során is könnyen elérhetőnek kell lenniük. Lehetőséget kell biztosítani a felhasználóknak arra, hogy a konkrét hozzájárulást a böngésző beállításain keresztül jelezzék. A magánélet védelmére vonatkozó preferenciák nem korlátozódhatnak a harmadik felek általi beavatkozásra vagy a sütitre. A munkacsoport határozottan javasolja a Do Not Track szabvány betartásának kötelezővé tételét.

A munkacsoport emellett további aggályos kérdéseket is azonosított, például a hatályra, a végberendezések védelmére és a közvetlen üzletszerzésre vonatkozóan. Végül, de nem utolsó sorban a munkacsoport olyan kérdéseket is azonosított, amelyek pontosításra szorulnak a végfelhasználók hatékonyabb védelme érdekében és a jogbiztonság növeléséhez minden érdekelt szereplő számára.

TARTALOM

1. BEVEZETÉS	6
2. A JAVASOLT RENDELET POZITÍVUMAI	6
<i>Az egész Unióra kiterjedő jogharmonizáció, a bírságok összehangolása, és az adatvédelmi hatóságokon keresztüli jogérvényesítés</i>	
<i>A hatály kiterjesztése az elektronikus hírközlési adatvédelmi irányelvhez képest</i>	<i>8</i>
<i>A jóváhagyási elvének célzott alkalmazása</i>	<i>11</i>
3. SÚLYOS AGGÁLYOK	11
<i>A javasolt rendelet csökkenti az általános adatvédelmi rendeletben biztosított védelem szintjét ..</i>	
4. TOVÁBBI AGGÁLYOK	19
<i>A rendelet területi és tárgyi hatályát ki kell bővíteni</i>	
<i>Fokozni szükséges a végberendezések védelmét</i>	<i>20</i>
<i>Közvetlen üzletszerzés</i>	<i>24</i>
<i>Menetrend</i>	<i>27</i>
<i>További aggályok</i>	<i>27</i>
5. A JOGBIZTONSÁGOT SZOLGÁLÓ PONTOSÍTÁSI JAVASLATOK	30
<i>A rendelet hatályára vonatkozó pontosítások</i>	
<i>A jóváhagyás fogalmának és alkalmazásának pontosítása</i>	<i>34</i>
<i>Tartózkodási helyre vonatkozó adatokkal és más metaadatokkal kapcsolatos pontosítások</i>	<i>35</i>
<i>Kéretlen közlésekkel kapcsolatos pontosítás</i>	<i>37</i>
<i>Az alapvető jogokat rögzítő jogi aktusok alkalmazásának pontosítása</i>	<i>38</i>
<i>Egyéb pontosítások</i>	<i>39</i>

1. BEVEZETÉS

1. A 29. cikk szerinti adatvédelmi munkacsoport (a továbbiakban: munkacsoport) üdvözlí az Európai Bizottság (EB) elektronikus hírközlési adatvédelmi rendeletre vonatkozó javaslatát (a továbbiakban: a javasolt rendelet, javasolt rendelet, elektronikus hírközlési adatvédelmi rendelet)¹, amelynek rendeltetése, hogy az elektronikus hírközlési adatvédelmi irányelv² helyébe lépjen.
2. A javasolt rendeletnek sok pozitív vonása van, és az Európai Bizottság a javasolt rendelet bemutatásával fontos lépést tett meg. A javasolt rendelet azonban tovább tökéletesíthető, ami nem csupán a végfelhasználók hatékonyabb védelmét, hanem a jogbiztonság növelését is szolgálná minden érdekelt szereplő számára.
3. A munkacsoport ennek megfelelően több aggályra és pontosítási javaslatra vár választ az Európai Parlament és a Miniszterek Tanácsa javasolt rendeletről folytatott vitájától. Ebben a véleményben elsőként a javasolt rendelet pozitív vonásait, majd az aggodalomra okot adó, illetve pontosításra szoruló kérdéseket vesszük számba.

2. A JAVASOLT RENDELET POZITÍVUMAI

AZ EGÉSZ UNIÓRA KITERJEDŐ JOGHARMONIZÁCIÓ, A BÍRSÁGOK ÖSSZEHANGOLÁSA, ÉS AZ ADATVÉDELMI HATÓSÁGOKON KERESZTÜLI JOGÉRVÉNYESÍTÉS

4. A munkacsoport üdvözlí, hogy a **szabályozási aktus a rendelet formáját ölti**. Ez biztosítja, hogy a szabályok (bizonyos kivételekkel, amelyekről az alábbiakban szó lesz) az Unió teljes területén egységesek legyenek. Biztosítja az áttekinthetőséget a felügyeleti hatóságok és a szervezetek számára. Emellett, tekintettel arra, hogy az általános adatvédelmi rendeletnek³ kulcsszerepe van a javasolt rendelet szempontjából, biztosítja a két jogi aktus összhangját. Emellett a **kiegészítő jogi aktus** alkalmazása (fenntartása) is pozitívum. A bizalmas közlés és a végberendezések védelmének olyan sajátosságai vannak, amelyekre az általános adatvédelmi rendelet nem tér ki. Az ilyen szolgáltatásokra vonatkozó kiegészítő rendelkezésekre ezért szükség van a közlések titkossága és a magánélet tiszteletben

¹ Javaslat az Európai Parlament és a Tanács rendeletére az elektronikus hírközlési ágazatban a magánélet tiszteletben tartásáról és a személyes adatok védelméről, valamint a 2002/58/EK irányelv hatályon kívül helyezéséről („Elektronikus hírközlési adatvédelmi rendelet”), 2017/0003 (COD), url: http://ec.europa.eu/newsroom/dae/document.cfm?doc_id=41241.

² Az Európai Parlament és a Tanács 2002/58/EK irányelve (2002. július 12.) az elektronikus hírközlési ágazatban a személyes adatok kezeléséről, feldolgozásáról és a magánélet védelméről (Elektronikus hírközlési adatvédelmi irányelv) (HL L 201., 2002.7.31., 37-47. o.), url: <http://eur-lex.europa.eu/legal-content/HU/TXT/?uri=celex:32002L0058>.

³ Az Európai Parlament és a Tanács (EU) 2016/679 rendelete (2016. április 27.) a természetes személyeknek a személyes adatok kezelése tekintetében történő védelméről és az ilyen adatok szabad áramlásáról, valamint a 95/46/EK irányelv hatályon kívül helyezéséről (általános adatvédelmi rendelet) (HL L 119/1., 2016.5.4., 1-88. o.), url: <http://eur-lex.europa.eu/legal-content/HU/TXT/?uri=CELEX%3A32016R0679>.

tartásához való alapvető jog megfelelő védelméhez. E tekintetben a munkacsoport határozottan támogatja a javasolt rendeletben választott, **széles körű tilalmakra és szűk kivételekre épülő elvi megközelítést**, és meggyőződése, hogy kerülni szükséges az általános adatvédelmi rendelet 6. cikke, és különösen a 6. cikk f) pontja szerinti, (jogos érdeken alapuló), általános jellegű kivételek bevezetését.

5. A két jogi aktus összhangját erősíti továbbá az is, hogy az e rendeletben foglalt szabályok érvényesítéséért **ugyanaz a hatóság felel, mint amely az általános adatvédelmi rendelet betartását felügyeli**. A személyes adatok védelme, illetve a bizalmas közlés és a végberendezések védelme közötti összefüggésre való tekintettel célszerű a javasolt rendeletben foglaltak érvényesítésével ugyanazt a felügyeleti hatóságot megbízni, mint az általános adatvédelmi rendelet érvényesítésével (javasolt rendelet (38) és (18) preambulumbekzdése). Az Európai Unió Bíróságának (EUB) joggyakorlata⁴ megerősíti továbbá annak alapvető fontosságát, hogy a felügyeleti hatóság a Charta 7. cikkében előírtaknak megfelelően független legyen. A gyakorlatban azonban ez jelentős többletmunkát jelenthet az adatvédelmi hatóságok számára, aminek teljesítésére a költségvetés növelése nélkül nincs garancia. Az adatvédelmi hatóságok ezért üdvözlík a javasolt rendelet (38) preambulumbekzdését, amely kiemeli, hogy minden felügyeleti hatóság számára biztosítani kell az új rendeletről eredő feladatok hatékony ellátásához szükséges plusz pénzügyi és humán erőforrásokat, létesítményeket és infrastruktúrát. Üdvözlendő továbbá, hogy a 18. cikk (2) bekezdése megteremti a jogalapot a javasolt rendelet szerinti felügyeleti hatóságok és az Európai Elektronikus Hírközlési Kódex létrehozásáról szóló, javasolt irányelv szerinti nemzeti szabályozó hatóságok között⁵.
6. Tekintettel a javasolt rendelet és az általános adatvédelmi rendelet közötti szoros kapcsolatra, **a két rendeletben előírt bírságok összehangolása** szintén üdvözlendő. A javasolt rendelet hatálya alá tartozó, többek között a bizalmas közlésbe és a végberendezésekbe történő beavatkozás révén megvalósított tevékenységek ige érzékeny jellegűek. A bírságok mértékét ennek megfelelően kell megállapítani. Ez az érzékeny jelleg az oka annak is, hogy miért fontos az Európai Unió teljes területére kiterjedő harmonizáció, a teljes régióban azonos, magas szintű védelem biztosítása. A javasolt rendelet 23. cikke egyes esetek kivételével (lásd a 38. megjegyzést) az általános adatvédelmi rendeletben foglaltak megsértéséért járó bírságok szintjéhez hasonló, megfelelő bírságokat ír elő a rendelet megsértése esetére.
7. Az **adatvédelmi incidensek bejelentésére vonatkozó konkrét szabályoknak** e jogi aktusból történő eltávolítása szintén üdvözlendő, mert ezzel elkerülhető az adatvédelmi incidensekre vonatkozóan az általános adatvédelmi rendeletben foglalt követelményekkel való szükségtelen átfedés.

⁴ Lásd pl. az EUB. C-362/14. sz. ügyben (*Safe Harbour*) 2015. október 6-án hozott ítéletének 41. pontját és az EUB C-203/15. és C-698/15. sz. ügyben (*Tele2/Watson*) 2016. december 21-én hozott ítéletének 123. pontját

⁵ Javaslat: Az Európai Parlament és a Tanács irányelve az Európai Elektronikus Hírközlési Kódex létrehozásáról (átdolgozás), 2016/0288 (COD), 2016.10.12., url: http://eur-lex.europa.eu/legal-content/HU/ALL/?uri=comnat:COM_2016_0590_FIN.

8. Üdvözlendő továbbá, hogy a **figyelem középpontjába a valamennyi végfelhasználó számára biztosítandó azonos szintű védelem került** azzal, hogy a javasolt rendelet már nem kíván különbséget tenni az előfizetők és az elektronikus kommunikációs szolgáltatások egyéb felhasználói között.

A HATÁLY KITERJESZTÉSE AZ ELEKTRONIKUS HÍRKÖZLÉSI ADATVÉDELMI IRÁNYELVHEZ KÉPEST

9. A munkacsoport üdvözlí a javasolt rendelet hatályának **kiterjesztését a hálózatsemleges online szolgáltatókra**, mint olyan szolgáltatásokra, amelyek működésük tekintetében a hagyományosabb hírközlési eszközökkel egyenértékűek, és ezért hasonló hatással lehetnek az uniós polgárok magánéletére és a közlések titkosságához való jogára. A munkacsoport kiemelten üdvözlí, hogy a rendelet hatálya a **hálózatsemleges online szolgáltatók** minden kategóriájára (OTT0, OTT1, az OTT2 egy része)⁶ kiterjed, mivel az nem csak a kommunikáció hagyományos eszközeire (OTT0), hanem a javasolt rendelet 8. cikk (1) bekezdés c) pontjában említett, funkcionálisan egyenértékű szolgáltatásokra (OTT1) is vonatkozik. Pozitívum továbbá, hogy a rendelet az Európai Elektronikus Hírközlési Kódexben foglalt fogalommeghatározásokon túl az OTT2 kategóriába tartozók egy részére is kiterjed, amennyiben azok a szolgáltatásaikhoz szorosan kötődő kiegészítő, személyközi, interaktív kommunikációs szolgáltatásokat is nyújtanak, például játékokban, társskereső alkalmazásokban vagy értékelő oldalakon (javasolt rendelet 4. cikkének (2) bekezdése). Üdvözlendő továbbá annak **tisztázása, hogy a védelem a gépek közötti interakcióra is kiterjed**. A (12) preambulumbekkezdés egyértelművé teszi, hogy az egymással kommunikáló berendezések is a javasolt rendeletben biztosított védelem hatálya alá tartoznak. Ez kívánatos, mivel az ilyen kommunikáció gyakran tartalmaz a magánélet védelméhez való jog által védett információkat. Ennek alkalmazása azonban pontosításra szorulhat (lásd a 40. megjegyzést).
10. Pozitívum továbbá, hogy a javasolt rendelet egyértelműen kiterjed a **tartalmakra és a kapcsolódó metaadatokra is**. A (14) preambulumbekkezdés egyértelművé teszi, hogy az „elektronikus kommunikációs adatok” 4. cikk (3) bekezdésének a) pontjában foglalt meghatározását kellően tágan szánták ahhoz, hogy minden tartalmat, valamint a kapcsolódó metaadatokat is magába foglalja, függetlenül például az adattovábbítás módjától. A munkacsoport azonban a 39. megjegyzésben aggodalommal jegyzi meg, hogy az „elektronikus kommunikációs adatok” e meghatározása még vita tárgya. A hatály kiterjesztésével összhangban a munkacsoport elengedhetetlenül fontos kiegészítésnek tartja annak **elismerését, hogy a metaadatok nagyon érzékeny adatokat fedhetnek fel** (lásd: indoklás 2.2 pontja; (2) preambulumbekkezdés). A munkacsoport üdvözlí, hogy ezzel az Európai Bizottság beépíti a Bíróság *Digital Rights Ireland* és *Tele2/Watson* ügyekben jelzett

⁶ A kifejezések részletesebb magyarázatát ld. itt: BEREC, *Report on OTT Services*, BoR (16) 35, 2016. január 29. 15. és 16. o., url: http://berec.europa.eu/eng/document_register/subject_matter/berec/reports/5751-berec-report-on-ott-services. Lásd továbbá a jelentésben található megjegyzést arra vonatkozóan, hogy a kategóriák nem jogi koncepciók, hanem a felülvizsgálatra vonatkozó vitában alkalmazandó fogalmak.

szempontjait. A munkacsoport üdvözli továbbá annak elismerését, hogy a **tartalmak elemzése nagy kockázattal járó adatkezelés**. A (19) preambulumbekkezdés és a 6. cikk (3) bekezdésének b) pontja rögzíti azt a logikus jogi vélelmet, hogy a tartalom átvizsgálása az általános adatvédelmi rendelet 35. cikke értelmében magas kockázattal járó adatkezelés, és a jelek szerint minden esetben előzetes egyeztetést igényel a (vezető) adatvédelmi hatósággal, függetlenül attól, hogy a fennmaradó kockázat szintje magas-e. A munkacsoport számára ugyanakkor aggodalomra ad okot a „metaadat” definíciója, és hogy a metaadatok elemzése esetében nem áll fenn hasonló kötelezettség adatvédelmi hatásvizsgálat elvégzésére (lásd a 33. és 46. megjegyzést).

11. Szintén üdvözlendő az **anonimizálás fontosságának további elismerése**. Az anonimizálási intézkedéseknek már az elektronikus hírközlési adatvédelmi irányelvben is szerepük volt az összeférhetőség biztosításában (az irányelv 6. cikke (1) bekezdése például rögzíti, hogy a forgalmi adatokat törölni kell, vagy anonimé kell tenni, ha a közlés továbbításához már nem szükségesek). A javasolt rendelet 6. cikke (2) bekezdésének c) pontja és 6. cikke (3) bekezdésének b) pontja jóváhagyás alapján lehetővé teszi a metaadatok kezelésének tilalma alóli kivételt, amennyiben az adott cél „anonimizált információ kezelésével nem teljesíthető”. Az ilyen, a magánélet védelmét szolgáló, a felhasználók jóváhagyásának kikérésén felül előírt intézkedések előírása védi ezeket a felhasználókat az indokolatlan adatkezeléstől. A munkacsoport ugyanakkor súlyosan aggályosnak találja, hogy az ilyen anonimizálási technikák alkalmazása nem lenne kötelező a felhasználók mozgásának mobil eszközeik segítségével történő követésénél (lásd a 17. megjegyzést). Emellett a szolgáltatóknak minden esetben el kellene végezniük az adatvédelmi hatásvizsgálatot, akkor is, ha anonimizálási intézkedést kell alkalmazniuk (lásd a 33. és 46. megjegyzést), és a munkacsoport szükségesnek tartja előírni az adatok anonimizálása és összesítése módjának közzétételét is (lásd a 42b megjegyzést).
12. További pozitív pont a **végberendezések védelmének széles körű megfogalmazása**. A (20) preambulumbekkezdés és a 8. cikk rögzíti, hogy a végberendezéshez való hozzáféréshez használt technológia lényegtelen: (bizonyos kivételekkel) a végberendezés működésébe való bármilyen beavatkozás, ideértve az adatfeldolgozási kapacitás igénybevételét is, a végfelhasználó jóváhagyását igényli. Hasznos, hogy az EB megerősítette, hogy az eszközazonosítás is e rendelkezés hatálya alá esik. A munkacsoport üdvözli továbbá, hogy amennyiben egy harmadik fél nem tartja be az érintett személy **böngészőbeállításokban** kifejezett preferenciáit, azok a (22) preambulumbekkezdésben írtak szerint **kikényszeríthetőek**. Ez hasznos azokban a helyzetekben, amikor egy harmadik fél, például egy hirdetési hálózat nem tartja tiszteletben a beállításokat. Ezt azonban rögzíteni kellene a javasolt rendelet egy ezzel foglalkozó rendelkezésében is.
13. Végül pedig üdvözlendő, hogy a **javasolt rendelet hatálya továbbra is kiterjed a jogi személyekre** (lásd: indoklás 2.2 pontja; (3), (33) és (42) preambulumbekkezdés; 1. és 15. cikk, 16. cikk (5) bekezdése). Ez már az elektronikus hírközlési adatvédelmi irányelvben is így van, de mivel az új szabályok érvényesítése az adatvédelmi hatóságok feladata lesz, hasznos ezt külön kiemelni. Ez lehetővé teszi az adatvédelmi hatóságok számára, hogy fellépjenek azokban az esetekben, amikor a jogsértés

áldozata jogi személy például a vállalatokhoz érkező levélszemét vagy a vállalati kommunikáció rejtett megfigyelése esetén. A munkacsoport azonban aggályosnak találja, hogy a jóváhagyás kérdése jogi személyek esetében nem világos (lásd a 41a megjegyzést), és hogy nem egyértelmű, hogy a közvetlen üzletszerzés esetében mit kell érteni a jogi személy „jogos érdeke” alatt (lásd a 43c megjegyzést).

14. A munkacsoport üdvözlí a jóváhagyás elvének alkalmazásához és értelmezéséhez kapcsolódó fejlesztéseket. Üdvözlendő elsőként **annak tisztázása, hogy az internet-hozzáférés és a (mobil)telefon-szolgáltatás alapvető szolgáltatás, és ezek nyújtói nem „kényszeríthetik” ügyfeleiket olyan adatkezeléshez való hozzájárulásra, amely magának az alapvető szolgáltatásnak a nyújtásához nem szükséges.** A (18) preambulumbekzdés kiemeli, hogy az alapszintű szélessávú internet-hozzáférés és a hang alapú kommunikációs szolgáltatások alapvető szolgáltatásnak tekintendők, ami azt jelenti, hogy mivel az emberek függenek az e szolgáltatásokhoz való hozzáféréstől, a kommunikációs adataiknak további célokra (pl. hirdetési vagy üzletszerzési célokra) történő kezelésére vonatkozó hozzájárulás nem lehet érvényes. A munkacsoport ugyanakkor tart attól, hogy ez a pontosítás túl korlátozott körű. Egyes hálózatsemleges online szolgáltatók által nyújtott szolgáltatások szintén alapvető szolgáltatásnak minősülhetnek, és az elektronikus hírközlési adatvédelmi rendeletnek más körülményekre vonatkozóan is kifejezetten meg kell tiltania a felhasználók „kell vagy nem?” jellegű választás elé állítását (lásd a 20. megjegyzést).
15. Pozitívum továbbá annak a **követelménynek a harmonizálása, hogy természetes személyek személyes adatai csak azok jóváhagyásával szerepeltethetők névjegyzékben.** A javasolt rendelet 15. cikke értelmében az adatok nyilvános névjegyzékekben történő kezelése természetes személyek esetében csak azok jóváhagyásával megengedett, jogi személyek esetén pedig lehetőséget kell biztosítani kifogás emelésére. Ezt a (31) preambulumbekzdés tovább részletezi azzal, hogy a jóváhagyást kifejezetten a névjegyzékben szerepeltetendő személyes adatok konkrét kategóriára vonatkozóan kell megadni. A munkacsoport aggodalommal jegyzi azonban meg, hogy a javasolt rendelet egyértelműbben rögzíthetné, hogy konkrét külön jóváhagyásra van szükség a kereséshez és az ellentétes irányú kereséshez (lásd a 37. megjegyzést).
16. A munkacsoport értékeli továbbá a **végberendezések működésébe történő nem zavaró beavatkozásra vonatkozó új, célzott kivételt is.** A munkacsoport hasznosnak találja, hogy a javasolt rendelet pontosítja, hogy a tilalom nem vonatkozik az internetes forgalom mérésére (a kivételt szűk körben határozva meg, mivel csak arra vonatkozik, ha a mérést a végfelhasználó által kért, információs társadalommal összefüggő szolgáltatást nyújtó szolgáltató végzi (lásd a javasolt rendelet 8. cikke (1) bekezdésének d) pontját). Lásd a (21) preambulumbekzdést is. A munkacsoport javasolja azonban a technológia szempontjából semlegesebb meghatározás használatát és a kivétel alkalmazhatóságának pontosítását (lásd a 25. megjegyzést).

3. SÚLYOS AGGÁLYOK

A JAVASOLT RENDELET CSÖKKENTI AZ ÁLTALÁNOS ADATVÉDELMI RENDELETBEN BIZTOSÍTOTT VÉDELEM SZINTJÉT

A fent említetteknek megfelelően a javasolt rendelet számos előrelépést tartalmaz. Felmerülnek azonban aggodalomra okot adó, eltérő súlyosságú kérdések is. Ebben a fejezetben a munkacsoport azt a négy kérdést ismerteti, amelyek **különösen nagy**

aggodalomra adnak okot. Olyan rendelkezésekről van szó, amelyek **csökkentik az általános adatvédelmi rendeletben biztosított védelem szintjét:**

17. A **rendelet végberendezések helyének nyomon követésére vonatkozó követelményeinek összhangban kell lennie az általános adatvédelmi rendelet követelményeivel.** A javasolt rendelet 8. cikke (2) bekezdésének b) pontja csupán tájékoztató kihelyezéséhez és biztonsági intézkedések alkalmazásához köti a végberendezések által kibocsátott információk gyűjtését. A 8. cikk (2) bekezdésének b) pontja megjegyzi továbbá, hogy az ilyen adatgyűjtésért felelős személynek jeleznie kell azokat a lépéseket, amelyek révén a végfelhasználók a minimálisra csökkenthetik vagy leállíthatják az adatok gyűjtését. A 8. cikk (2) bekezdésének b) pontja ezzel azt a benyomást kelti, hogy a szervezetek az érintett személy jóváhagyása nélkül is gyűjthetik a végberendezések által kibocsátott információkat az egyének fizikai mozgásának nyomon követése céljából (például wifi vagy bluetooth alapú nyomon követéshez). Az adatokat gyűjtő fél a jelek szerint eleget tesz az előírásoknak azzal, ha tájékoztatót helyez ki a felhasználók számára arról, hogy kapcsolják ki a készülékeiket, ha nem szeretnék, hogy nyomon kövessék őket. Ez a megközelítés ellentétes lenne az Európai Bizottság távközlési politikájának alapvető céljával, azaz azzal, hogy alacsony költségek és magas szintű adatvédelem mellett nagy sebességű, a határokon átnyúló mobil internetkapcsolatot biztosítson minden európai számára.

A javasolt rendelet emellett nem szab egyértelmű korlátokat a gyűjtött adatok körére és az adatok azt követő kezelésére vonatkozóan sem. Ezzel kapcsolatban meg kell jegyezni, hogy a MAC-címek személyes adatok, még akkor is, ha biztonsági műveleteket, például hasítást végeztek rajtuk. További követelmények vagy korlátok előírása nélkül a javasolt rendelet jelentősen alacsonyabb szintű védelmet biztosít a személyes adatok számára, mint az általános adatvédelmi rendelet, amelynek értelmében az ilyen nyomon követésnek tisztességesnek és törvényesnek, valamint átláthatónak kell lennie. A (25) preambulumbekkezdés sem segít annak megjegyzésével, hogy a wifijelek nyomon követésére szolgáló funkciók egy része nem jár magas adatvédelmi kockázattal, míg mások, például az egyének hosszabb időn keresztül történő nyomon követése, magas adatvédelmi kockázatot jelent. A munkacsoport értékeli annak elismerését, hogy az utóbbi nagy adatvédelmi kockázattal jár, de nem hasznos azt előre, az adatkezelés körülményeinek és arányosságának további vizsgálata nélkül eldönteni, hogy bizonyos más funkcióknak nincs ilyen kockázata. Az erre vonatkozó vizsgálat során a wifijelek nem anonimizált nyomon követésével kapcsolatban az alábbi feltételeket kell figyelembe venni.

Az adatgyűjtés körülményeitől és céljától függően az ilyen adatgyűjtés az általános adatvédelmi rendelet szerint várhatóan csak hozzájárulás birtokában, vagy csak abban az esetben folytatható, ha a gyűjtött személyes adatokat anonimizálják. Az anonimizálást lehetőség szerint azonnal az adatok begyűjtését követően kell elvégezni. Ha az adatgyűjtés célja nem teszi lehetővé az azonnali anonimizálást, annak elvégzéséig az adatok feldolgozása csak az alábbi feltételek mellett engedélyezett: i. az adatgyűjtés célja pusztán statisztikai számlálásra korlátozódik (lásd az alábbi példákat); ii. a nyomon követés térben és időben az adott célhoz feltétlenül szükséges mértékre szorítkozik; iii. az adatokat közvetlenül utána törlik

vagy anonimizálják, és iv. tényleges kívülmaradási lehetőség áll rendelkezésre. Az adatkezelőnek természetesen minden esetben eleget kell tenni a megfelelő tájékoztatás nyújtására vonatkozó követelménynek.

A munkacsoport tart attól, hogy amennyiben az ilyen adatokat gyűjtő szervezetek külön-külön ajánlják fel az adatgyűjtésben való részvétel elutasításának lehetőségét, az elfogadhatatlan terhet jelentene a polgárok számára, tekintve, hogy a magán- és az állami szektorbeli szervezetek egyre növekvő mértékben alkalmazzák ezeket a nyomonkövetési technológiákat. A munkacsoport ezért felkéri az európai jogalkotót, hogy ösztönözze az olyan műszaki standardok kidolgozását, amelyek révén a berendezések képesek automatikusan jelezni a nyomonkövetés el nem fogadását, és biztosítsa az ilyen jelzés figyelembevételének kikényszeríthetőségét.

Az általános adatvédelmi rendelet értelmében például valószínűleg beleegyezés szükséges ahhoz, hogy az adatkezelő az eszközök közvetetten azonosítható (wifi vagy bluetooth) MAC-címét begyűjtés és rögzítse, és kiszámítsa a felhasználó helyét azért hogy nyomon követhesse a felhasználó tartózkodási helyének változtatását az idő múlásával, például több üzletben. Különösen így van ez abban az esetben, ha a nyomon követés közterületen történik, ahol a felhasználók jogosan számítanak arra, hogy nem azonosítják vagy követik nyomon őket, ám a járókelők MAC-címét mégis gyűjtik. A jóváhagyás ilyen esetben megadható például egy alkalmazás segítségével, amely felkéri a felhasználókat, hogy kereskedelmi ajánlatokért cserébe meghatározott területeken engedélyezzék a tartózkodási helyük nyomon követését; meghatározott helyeken belül elhelyezkedő bejelentkezési pontok felkínálásával; vagy a vezeték nélküli internet-hozzáférési pontba épített jóváhagyás-kezelő modul révén.

Korlátozott azon körülmények száma, amelyek fennállása esetén az adatkezelő számára az érintett személy beleegyezése nélkül is engedélyezett a végberendezések által kibocsátott információk feldolgozása azok mozgásának követése céljából. Ide tartozhat például az adott helyen található vevők megszámlálása, vagy ha a várakozási idő kijelzése céljából gyűjtik a biztonsági beléptető pont két oldalán kibocsátott jeleket. Mindkét példa esetében azonban az adatokat azonnal törölni vagy anonimizálni kellene, amint azok statisztikai célja teljesült. Ez azt jelenti, hogy az egy adott helyen, például egy üzletben tartózkodó látogatók készülékeinek MAC-címét a begyűjtést követően azonnal anonimizálni kellene, azok tartós tárolása nélkül, olyan módon, hogy az újbóli azonosítás műszakilag kizárható legyen. A várakozási idő kiszámítása esetében a MAC-címet azonnal törölni vagy anonimizálni kellene, amint nincs már rá szükség a várakozási idő kiszámításához, például mert a látogató átért a biztonsági beléptető pont másik oldalára, vagy elhagyta a sort.

Az adatkezelőnek emellett eleget kellene tennie az adatgyűjtés minimalizálására vonatkozó követelményeknek is (az adatgyűjtés például nem lehet folyamatos, ha annak célja az üzletek nyitvatartására és/vagy időszakos mintavételre korlátozódik). Az adatkezelőnek további enyhítő intézkedéseket is kell tenniük annak biztosítására, hogy a tevékenység ne vagy csak kis mértékben zavarja a felhasználók magánélethez való jogát, például az adatgyűjtés helyének közelében lakók magánéletének védelme érdekében.

Az, hogy a javasolt rendelet 8. cikkének (2) bekezdésében foglalt követelmény csupán tájékoztatás kihelyezésére korlátozódik, különösen figyelemre méltó a (20) preambulumbekkezdés fényében, amely megállapítja, hogy a végfelhasználók berendezéseivel összefüggő információk azonosítás és nyomon követés céljából történő gyűjtése távolból is történhet, és hogy az ilyen adatkezelés a javasolt rendelet értelmében súlyosan sértheti az ilyen végfelhasználók magánélet védelméhez való jogát. Ez a követelmény továbbá nem megy túl az általános adatvédelmi rendelet 13. és 14. cikkében már rögzített tájékoztatási kötelezettségen. A magánéletbe való súlyos beavatkozást, amit a nyomon követés jelent, tovább súlyosbítja, hogy az összegyűjtött adatokhoz potenciálisan mások is hozzáférhetnek: így például a bűnüldöző szervek a mobil készülékek által sugárzott, eltárolt MAC-cím(ek) alapján azonosíthatják a végfelhasználókat.

18. Szükség van a tartalmak és a metaadatok elemzésére vonatkozó feltételek részletesebb meghatározására.

A javasolt rendelet 6. cikke eltérő szintű védelmet biztosít a metaadatok, illetve a tartalmak számára. A munkacsoport nem támogatja ezt a különbségtételt: mindkét kategóriába tartozó adatok kiemelten érzékenyek. A metaadatok és a tartalmak számára ezért egyformán magas szintű védelmet kell biztosítani. A kiindulási pontnak tehát annak kell lennie, hogy a metaadatokat és a tartalmat egyaránt tilos feldolgozni, amíg ahhoz valamennyi végfelhasználó hozzá nem járult (azaz küldők és címzettek egyaránt).

Az elérni kívánt céltól függően azonban bizonyos adatkezelés hozzájárulás nélkül is végezhető, amennyiben az az adott célhoz feltétlenül szükséges:

- A szolgáltatók számára engedélyezett az elektronikus kommunikációs adatok feldolgozása a javasolt rendelet 6. cikke (1) bekezdésének a) és b) pontjában, valamint a 6. cikke (2) bekezdésének a) és b) pontjában említett célokból⁷.
- Tisztázni kell, hogy bizonyos, a kérértlen üzenetek felismerésére és kiszűrésére, illetve bothálózatok működésének akadályozására szolgáló technikák szintén feltétlenül szükségesnek tekinthetők az elektronikus hírközlési szolgáltatások visszaélészerű használatának felismeréséhez és megakadályozásához (6. cikk (2) bekezdésének b) pontja). A kérértlen üzenetek kiszűrése terén az ilyen üzeneteket kapó végfelhasználóknak, amennyiben műszakilag lehetséges, több szintű lehetőséget kell biztosítani a szolgáltatás visszautasítására.
- Tisztázni kell, hogy az elektronikus kommunikációs adatok ügyfélszolgálati célokra történő elemzése is a „számlázáshoz szükséges” kivétel alá eshet (lásd: 6. cikk (2) bekezdésének b) pontja). Az erre vonatkozó metaadatok

⁷ Ami a szolgáltatás minőségére vonatkozó kötelező követelmények betartását illeti, a szolgáltatóknak a javasolt rendelet 6. cikke (2) bekezdésének a) pontjában foglaltaknak megfelelően figyelembe kell venniük a 15/2120/EU rendeletben (az Európai Elektronikus Hírközlési Kódexben), konkrétan annak 3. cikkében és a 10., valamint (13)-(15) preambulumbekkezdésében foglalt feltételeket. E rendelkezés alapján a szolgáltatókkal szemben követelmény lehet a kommunikációs adatok feldolgozása annak érdekében, hogy felismerjék és kiszűrjék a rosszindulatú tartalmakat és kémprogramok, továbbá engedélyezett lehet számukra az adatok tömörítése.

azon időszak végéig őrizhető meg, amíg a számla ellen jogszerűen kifogás emelhető, illetve amíg a számla teljesítése a nemzeti jog alapján követelhető. A kapcsoló adatok (például URL-címek) csak a végfelhasználói kérésére őrizhető meg, és akkor is csak a számlával kapcsolatos vita rendezéséhez feltétlenül szükséges ideig (ami azt jelenti, hogy a 7. cikk (3) bekezdését ennek megfelelően kell módosítani).

- Lehetővé kell tenni az elektronikus kommunikációs adatoknak a végfelhasználó által kifejezetten kért szolgáltatások (például keresés, kulcsszó alapú indexálás, virtuális asszisztensek, szövegfelolvasás, fordítás) céljára történő kezelését. Ehhez be kell vezetni egy olyan kivételt, amely lehetővé teszi az ilyen adatok tisztán egyéni (otthoni) célra, valamint egyéni munkavégzés céljára történő elemzését⁸. Ez tehát lehetővé tenné az elemzés valamennyi végfelhasználó jóváhagyása nélkül, azonban a szolgáltatást kérő végfelhasználó beleegyezésével történő elvégzését. Az ehhez szükséges specifikus jóváhagyás egyben azt is kizárná, hogy a szolgáltató más célra használja fel ezeket az adatokat.

Ez azt jelenti, hogy a tartalmak és/vagy a metaadatok bármilyen más, például elemzési, profilalkotási, viselkedés alapú hirdetési vagy egyéb, a szolgáltató (kereskedelmi) érdekeit szolgáló céllal végzett elemzéséhez valamennyi olyan végfelhasználó beleegyezése szükséges, akiknek az adatait feldolgozzák. Az ilyen helyzetek tekintetében a javasolt rendeletnek rögzíteni kell, hogy önmagában egy elektronikus levél vagy egyéb személyes közlés másik szolgáltatásból történő elküldése egy olyan végfelhasználónak, aki személy szerint beleegyezett saját tartalmainak és metaadatainak kezelésébe (például a levelezési szolgáltatás megrendelése során), nem minősül a feladó által adott érvényes jóváhagyásnak.

Végül pedig tisztázni kell, hogy a végfelhasználóktól eltérő személyek adatainak (például harmadik személy fényképének vagy leírásának, amely két személy közötti üzenetváltásban szerepel) kezelése szintén meg kell hogy feleljen az általános adatvédelmi rendelet megfelelő rendelkezéseinek.

19. **A végberendezéseknek és a szoftvereknek *alapértelmezettként* meg kell nehezíteniük, akadályozniuk és meg kell tiltaniuk a működésükbe való jogellenes beavatkozást, és tájékoztatást kell nyújtaniuk a lehetőségekről.** Bár a javasolt rendelet kötelezi az elektronikus kommunikációt lehetővé tevő szoftverek nyújtóit arra, hogy lehetőséget biztosítsanak a végberendezések működésébe való korlátozott beavatkozás megakadályozására, és hogy a telepítést követően a végfelhasználó jóváhagyását kérjék a beállításokhoz (10. cikk (1) és (2) bekezdése), ez a választási lehetőség nem azonos az *alapértelmezett adatvédelemmel*. Emellett a meghatározott beavatkozások megakadályozásának lehetősége már jelenleg is létezik, de eddig nem

⁸ Bár a javasolt rendelet (13) preambulumbekkezdés kifejezetten kizárja a vállalati hálózatokat a rendelet hatálya alól, ebben az új, egyéni felhasználásra vonatkozó kivételben ki kell térnie arra az esetre, amikor a munkavállalók munkájukhoz kapcsolódóan, például az elektronikus levelek között végzett kereséshez vesznek igénybe felhő alapú szolgáltatásokat.

vezetett a szükségtelen nyomon követés elleni kellő mértékű fellépéshez. Pontosan ez az oka annak, hogy az általános adatvédelmi rendeletben tudatos szakpolitikai döntésként került bevezetésre a beépített és alapértelmezett adatvédelem és magánélet-védelem elve (általános adatvédelmi rendelet 25. cikke). A javasolt rendelet a hírközlési adatok és a berendezések adatai tekintetében ellentétes ezekkel az elvekkel. A ((10) preambulumbekzdésben említett) rádióberendezésekről szóló 2014/53/EU irányelv⁹ eközben csak nagyon korlátozott követelményt ír elő a biztonság terén azzal, hogy a rádióberendezések „biztonsági berendezéseket tartalmaznak a felhasználó és az előfizető személyes adatainak és magánéletének védelmére” (3. cikk (3) bekezdésének e) pontja). Ez nem helyettesítheti az alapértelmezett adatvédelmi beállításokra vonatkozó konkrét követelményeket a javasolt rendeletben. Ezzel kapcsolatban érdemes megjegyezni, hogy az Eurobarometer elektronikus adatvédelemre vonatkozó, 2016 decemberében közzétett felmérésében „[t]íz válaszadó közül közel hét (69 %) teljesen egyetértett azzal, hogy a böngésző alapértelmezett beállításainak meg kell akadályozniuk az adataik megosztását”¹⁰. A munkacsoport külön pontban tárgyalja a böngészők beállításait és a „harmadik felek” definíciójával kapcsolatos aggályát. Lásd a 24. megjegyzést. Nem szabad megfeledkezni továbbá arról, hogy ez a rendelkezés nem csak a számítógépeken használt böngészőket érinti, hanem kiterjed minden egyéb típusú szoftverre is, amely kommunikációt tesz lehetővé (ideértve az operációs rendszereket, az alkalmazásokat és a tárgyak internetéhez kapcsolódó eszközök illesztési felületét biztosító szoftvereket). Összességében tehát a végberendezéseknek és a szoftvereknek *alapértelmezettként* a magánélet védelmét biztosító beállításokat kell nyújtaniuk, és útmutatást kell kínálniuk a felhasználó számára a konfigurációs menük használatához, ha a telepítés során el kívánnak térni ezektől az alapértelmezett beállításoktól. A konfigurációs menünek az üzemeltetés során is bármikor könnyen elérhetőnek kell lennie. A munkacsoport arra kéri az európai jogalkotót, hogy ennek megfelelően pontosítsa a 10. cikk hatályát.

- 20. Az elektronikus hírközlési adatvédelmi rendeletnek kifejezetten meg kell tiltania a hozzáférés feltételül szabott nyomon követési hozzájárulást,** azaz azt a gyakorlatot, hogy a honlaphoz vagy szolgáltatáshoz való hozzáférés feltételül szabják az adott személy hozzájárulását a más weboldalakon vagy szolgáltatásokban történő nyomonkövetéshez. Amint a munkacsoport elektronikus hírközlési adatvédelmi irányelvre vonatkozó korábbi véleményeiben¹¹ is szerepel, az ilyen „kell vagy nem?” jellegű megoldások ritkán indokoltak¹². Ha végberendezések adatfeldolgozási és tárolási kapacitásának igénybevétele vagy a végfelhasználók végberendezéseiből gyűjtött információk lehetővé teszik a felhasználó adott

⁹ 2014/53/EU irányelv a rádióberendezésekről.

¹⁰ Lásd: Eurobarometer 443. gyorsfelmérés, Jelentés az elektronikus adatvédelemről (közzétéve 2016. december), 5. o.

¹¹ Lásd pl.: WP240 (elektronikus hírközlési adatvédelem áttekintése), 16. o.; WP 208 (mentességek a beleegyezési követelmény alól), 5. o.

¹² Ez az álláspont nem sérti az általános adatvédelmi rendelet 7. cikkének (4) bekezdésében foglaltakat, amely szintén megtilthatja a „kell vagy nem?” jellegű választás elé állítást más, megfelelő esetekben.

időszakban vagy eszközökön (például különböző weboldalakon és alkalmazásokban) folytatott tevékenységeinek nyomon követését, az ilyen adatok kezelése súlyosan sértheti az érintett felhasználó magánéletét. Tekintve az internetnek a szólásszabadsághoz való alapvető jog érvényesülésében játszott alapvető fontosságát, ideértve az információkhoz való hozzáférés jogát, az online tartalmakhoz való hozzáférésnek nem lehet feltétele az, hogy az egyén hozzájárulását adja a különböző eszközökön, weboldalakon vagy alkalmazásokban folytatott tevékenysége nyomon követéséhez. Az eljövendő elektronikus hírközlési adatvédelmi rendeletnek ezért rögzítenie kell, hogy az ilyen, erősen zavaró adatkezeléshez való hozzájárulás nem szabható a tartalmakhoz, például weboldalakhoz vagy alkalmazásokhoz való hozzáférés feltételül, függetlenül a nyomon követéshez használt technológiától, történjen az sütikkel, eszközazonosítással, egyedi azonosítók beillesztésével vagy más megfigyelési módszerrel. Ennek a tiltásnak a szükségességére mutat rá az elektronikus adatvédelem témakörében a közelmúltban elvégzett Eurobarometer-felmérés, amely szerint „[a] válaszadók közel kétharmada (64 %) szerint elfogadhatatlan, hogy egy adott honlaphoz való korlátlan hozzáférést cserébe megfigyeljék az online tevékenységeiket”.

21. Összegzőként: a fent említett négy kérdés esetében a **javasolt rendeletnek teljesítenie kell azt az ígértét, hogy az általános adatvédelmi rendelettel azonos, vagy annál magasabb szintű védelmet biztosít.** Az (5) preambulumbekkezdés tényként állítja, hogy a javasolt rendelet nem csökkenti az általános adatvédelmi rendeletben biztosított védelem szintjét. A javasolt rendelet jelenlegi állapotában azonban ez nem felel meg a valóságnak, különösen, ami az eszközök nyomon követését (17. megjegyzés) és az alapértelmezett adatvédelmet (19. és 18. megjegyzés) illeti. Ez különösen fontos azért, mert, amint azt ugyanaz a preambulumbekkezdés megjegyzi, a javasolt rendelet „az általános adatvédelmi rendelethez kapcsolódó, azt a személyes adatnak minősülő elektronikus kommunikációs adatok tekintetében részletező és kiegészítő *lex specialis*”. A munkacsoport javasolja, hogy az elektronikus hírközlési adatvédelmi rendelet szövege tegye egyértelművé legalább a következőket:

- i. az elektronikus hírközlési adatvédelmi rendeletben foglalt tilalmak erősebbek az általános adatvédelmi rendeletben foglalt engedélyeknél (pl. az elektronikus hírközlési adatvédelmi rendelet 5. cikkében szereplő beavatkozás tilalma erősebb, mint az elektronikus hírközlési szolgáltatást nyújtó szolgáltatók általános adatvédelmi rendelet 5. cikke (1) bekezdésének b) pontjában és 6. cikke (4) bekezdésében foglalt jogai a személyes adatok további feldolgozására);
- ii. ahol az elektronikus hírközlési adatvédelmi rendeletben foglalt tilalmak alóli kivétel (ideértve a jóváhagyást is) lehetővé teszi az adatok kezelését, az adatkezelésnek, amennyiben személyes adatokat érint, továbbra is meg kell felelnie az általános adatvédelmi rendelet vonatkozó rendelkezéseinek;
- iii. ahol az elektronikus hírközlési adatvédelmi rendeletben foglalt tilalmak alóli kivétel lehetővé teszi az adatkezelést, az általános adatvédelmi rendelet alapján történő minden más adatkezelés tiltott, beleértve az általános adatvédelmi rendelet 6. cikkének (4) bekezdése szerinti eltérő célú adatkezelést is. Ez nem akadályozza meg az adatkezelőket abban, hogy további jóváhagyást kérjenek az új adatkezelési műveletekhez. Azt sem

akadályozza meg, hogy a jogalkotók további, korlátozott, specifikus kivételeket fogalmazzanak meg az elektronikus hírközlési adatvédelmi rendeletben, például az általános adatvédelmi rendelet 89. cikke szerinti tudományos vagy statisztikai célú, vagy az általános adatvédelmi rendelet 6. cikk d) pontja szerinti, az egyének létfontosságú érdekeinek védelmét szolgáló adatkezelés engedélyezése céljából.

Az elektronikus hírközlési adatvédelmi rendeletet úgy kell továbbá értelmezni, hogy legalább ugyanolyan szintű, adott esetben pedig magasabb szintű védelmet nyújtson, mint az általános adatvédelmi rendelet.

4. TOVÁBBI AGGÁLYOK

A fent említetteken túl a 29. cikk szerinti munkacsoport **aggodalommal** jegyzi meg az alábbiakat.

A RENDELET TERÜLETI ÉS TÁRGYI HATÁLYÁT KI KELL BŐVÍTENI

22. A „metaadat” fogalmának meghatározása túl szűk körű. A fogalom jelentése a jelenlegi, 4. cikk c) pontjában található meghatározás szerint: „az elektronikus hírközlés tartalmának továbbítása, terjesztése vagy cseréje céljából elektronikus hírközlő hálózatban kezelt adatok” (utólagos kiemelés). A „hálózat” szó használata mintha arra utalna, hogy csak a hálózat „alsóbb” rétegeiben történő szolgáltatásnyújtás során létrejött adatok minősülnek metaadatnak. Ez azt jelentheti, hogy egy hálózatsemleges szolgáltatás nyújtása során létrejött adatok nem tartoznának a rendelet hatálya alá. Ez nemkívánatos lenne, és valószínűleg nem is ez volt a szándék, tekintve, hogy a javasolt rendelet hatályát ki kívánták terjeszteni a hálózatsemleges szolgáltatásokat nyújtó szolgáltatókra. Ennek orvoslásához az „elektronikus kommunikációs metaadatok” meghatározását úgy kellene módosítani, hogy az elektronikus hírközlés tartalmának továbbítása, terjesztése vagy cseréje céljából kezelt minden adatot magába foglaljon.

23. Aggályos továbbá, hogy a **javasolt rendelet területi hatálya az Unióban tevékenységi hellyel nem rendelkező szervezetek tekintetében csak az elektronikus hírközlési szolgáltatókat érinti**. A javasolt rendelet előírja, hogy az Unióban tevékenységi hellyel nem rendelkező elektronikus hírközlési szolgáltatóknak írásban ki kell jelölniük egy Unión belüli képviselőt (3. cikk (2) bekezdése). A (9) preambulumbekkezdés azt is említi, hogy a rendelet hatálya az elektronikus hírközlési szolgáltatók által végzett adatkezelésre az adatfeldolgozás helyétől függetlenül kiterjed. A munkacsoport üdvözlí ennek egyértelműsítését. Miután azonban a szövegben csak az elektronikus hírközlési szolgáltatók szerepelnek, bizonytalan, hogy a rendelet területi hatálya mennyiben terjed ki más típusú felekre (például a végfelhasználók végberendezései által sugárzott információkat gyűjtő vagy abba beavatkozó felekre – lásd a javasolt rendelet 3. cikke (1) bekezdésének c) pontját és 8. cikkét). A munkacsoport ezért javasolja a 3. cikk (2) és (5) bekezdésének módosítását oly módon, hogy azok a nyilvánosan elérhető névjegyzékek szolgáltatóira, az elektronikus kommunikációt lehetővé tévő szoftverek nyújtóira, a közvetlen üzletszerzési célú kereskedelmi közléseket küldő személyekre és a

végfelhasználók végberendezéseivel összefüggő, illetve azokon tárolt (egyéb) információk gyűjtőire is kiterjedjenek, amennyiben azok tevékenysége az Unióban tartózkodó személyekre irányul (lásd a javasolt rendelet (8) preambulumbekzdését).¹³

FOKOZNI SZÜKSÉGES A VÉGBERENDEZÉSEK VÉDELME

Az aggályok egy másik csoportja ahhoz kapcsolódik, hogy a javasolt rendelet nem biztosít kellő védelmet a végberendezések számára.

24. Az első probléma az, **hogy a javasolt rendelet tévesen azt sugallja, hogy nem specifikus böngészőbeállítások útján is érvényes beleegyezés adható.** A munkacsoport tisztában van azzal a szemponttal, hogy a végfelhasználókat jelenleg túlterheli a jóváhagyás iránti kérelmek nagy száma ((22) preambulumbekzdés). Ennek a problémának a megoldásában a böngészők (és más hasonló szoftverek) beállításai játszhatnak szerepet. Az általános böngészőbeállításokat azonban nem arra szánták, hogy egyedi alapon szabályozzák a nyomon követéshez használt technológiák alkalmazását, ezért nem alkalmasak az általános adatvédelmi rendelet 7. cikke és (32) preambulumbekzdése szerinti hozzájárulás megadásához (mivel a hozzájárulás nem megfelelő tájékoztatáson alapul, és nem kellően specifikus).

A végfelhasználónak képesnek kell lennie arra, hogy honlaponként vagy alkalmazásonként külön-külön hozzájárulást adjon különböző célokra (például a közösségi médiában történő megosztásra vagy reklámozásra). Ha egy adatkezelő több honlapért vagy alkalmazásért is felel, akkor a hozzájárulást kérheti az irányítása alatt álló valamennyi honlapra vagy alkalmazásra vonatkozóan is, feltéve, hogy ezt a kérést külön adja elő.

Az adatkezelőnek emellett a hozzájárulásra vonatkozó minden egyéb kötelezettségnek is eleget kell tennie, ideértve a felhasználók megfelelő tájékoztatására vonatkozó kötelezettséget is. Ez a böngészők és az adatkezelők esetében is azt jelenti, hogy csupán egyetlen, „minden süti elfogadása” opció felkínálása érvénytelen lenne, hiszen ez nem tenné lehetővé a felhasználók számára a kellő felbontású jóváhagyás megadását. A böngészőknek azonban lehetővé kell tenniük azt is, hogy a felhasználó megfelelő információk birtokában, tudatosan minden süti elfogadása mellett döntsön, és ezzel megakadályozza, hogy a továbbiakban felkeresett honlapoktól specifikus hozzájárulás iránti kérést kapjon.

A munkacsoport erősen javasolja, hogy az elektronikus hírközlési adatvédelmi rendelet tegye kötelezővé a böngészők számára olyan műszaki mechanizmus, például a Do Not Track szabvány alkalmazását, amely biztosítja, hogy a felhasználók valódi

¹³ Lásd az általános adatvédelmi rendelet 3. cikkének (2) bekezdését: „E rendeletet kell alkalmazni az Unióban tartózkodó érintettek személyes adatainak az Unióban tevékenységi hellyel nem rendelkező adatkezelő vagy adatfeldolgozó által végzett kezelésére, ha az adatkezelési tevékenységek: a) áruknak vagy szolgáltatásoknak az Unióban tartózkodó érintettek számára történő nyújtásához kapcsolódnak, függetlenül attól, hogy az érintettnek fizetnie kell-e azokért; vagy b) az érintettek viselkedésének megfigyeléséhez kapcsolódnak, feltéve hogy az Unió területén belül tanúsított viselkedésükről van szó.” Ez alól szintén engedélyezhetők az általános adatvédelmi rendelet 27. cikkének (2) bekezdéséhez hasonló kivételek.

döntési lehetőséggel és kontrollal rendelkezzenek az eszközeik működésébe való beavatkozás tekintetében¹⁴.

Még ennél is fontosabb, hogy az elektronikus hírközlési adatvédelmi rendelet biztosítsa, hogy mind az információ adott eszközön történő tárolására vonatkozó beállítást, mind a böngésző DNT jelét minden adatkezelő elfogadja a jóváhagyás/elutasítás kötelező jogilag kötelező kifejezéseként. Ez nem zárja ki, hogy a munkacsoport további útmutatást adjon ki a DNT szabványban foglaltak betartásáról, többek között a célhoz kötöttség elvének való megfelelésről, miután a szabvány (a tervek szerint 2017 végéig) véglegesítésre kerül.

A hozzájárulás közvetett formái, például a honlapra való kattintás vagy az oldal görgetése nem írhatja felül az adattárolásra vagy a DNT jelre vonatkozó beállítást. E szabvány használatának fontos előnye, hogy nem korlátozódik a sütiket alkalmazó nyomon követési technológiára, hanem a nyomonkövetés más formái, például az eszközazonosítás esetén is alkalmazható.

A szabvány betartásának jogszabályban történő előírása megoldja azt a másik problémát is, amelyet jelenleg a „harmadik felek” kifejezés 10. cikkben való szerepeltetése vet fel. Egy weboldal vagy egy alkalmazás általában sok elemből áll, amelyek egy része magához a webhelyhez tartozik, egy másik része pedig külső eredetű. A meglátogatott honlapon olyan külső kód is futhat, amelyik egy harmadik fél szerverére küld jelentést. Amikor például egy felhasználó felkeres egy közösségi oldalt, az első féltől egy nyomon követésre szolgáló sütit kaphat. Ugyanez a közösségi oldal harmadik fél lehet akkor, amikor a felhasználó egy másik honlapot keres fel, amely az említett közösségi oldallal való interakciót tartalmaz. Minden ilyen esetben, függetlenül attól, hogy a végfelhasználó készülékén tárolt adathoz való „hozzáférésről” vagy ott történő „adattárolásról” van-e szó, ez a készülék működésébe való beavatkozásnak minősül, amelyhez (valamely kivétel fennállásának kivételével) jóváhagyás szükséges. A DNT szabvány ezt adott honlapra, illetve az egész internetre vonatkozó beállításként különbözteti meg. Ezért a jogbiztonság valamennyi érdekelt számára történő növelése érdekében az elektronikus hírközlési adatvédelmi rendelet „harmadik felekre” való hivatkozását úgy kellene átfogalmazni, hogy magában foglaljon minden olyan felet, amellyel a berendezés interakcióba lép (vagy mert az adatot tárol a berendezésen, vagy mert az ott tárolt adathoz fér hozzá).

Ahhoz, hogy a Do Not Track szabvány kompatibilis legyen a közlések titkossága és az adatok számára a Charta által előírt magas szintű védelemmel, az elektronikus hírközlési adatvédelmi rendeletnek rögzítenie kell, hogy a nem egy adott honlapra, hanem az egész internetre kiterjedő nyomon követésre vonatkozó kéréseket külön kell előadni, és biztosítani kell, hogy a felhasználók szabadon elfogadhassák vagy elutasíthassák az ilyen kéréseket. A felhasználóknak a hozzájárulás iránti gyakori kérésekkel szembeni védelme érdekében az elektronikus hírközlési adatvédelmi rendeletnek azt is biztosítania kell, hogy amennyiben a felhasználó egy adott szervezet egész internetre vonatkozó nyomonkövetési kérését (akár a Do Not Track szabvány segítségével, akár külön feketelista útján) elutasította, az adott szervezet

¹⁴ Lásd itt: <https://www.w3.org/TR/tracking-compliance/>. A 7. pont ismerteti a kivételeket, valamint az adott honlapra és az egész világhálóra vonatkozó kivételek közötti különbséget. A 6. bekezdés tartalmazza azokat a gép által olvasható információkat, amelyeket az adatkezelők a hozzájárulás megszerzéséhez kapcsolódó tájékoztatási kötelezettség keretében rendelkezésre bocsáthatnak.

legalább 6 hónapon keresztül ne küldhessen hozzájárulás iránti újabb kérést. Ez a szabály nem zárja ki azt, hogy amennyiben a felhasználó közvetlenül felkeresi az adott szervezet honlapját, a szervezet (első félként) a saját honlapján kérelmet (azaz egy adott honlapra vonatkozó kérelmet) küldjön a felhasználónak. A gyakorlatban ez azt jelenti, hogy például egy videostreaming oldal, amely nyomon követést segítő sütiket küld, küldhet erre vonatkozó kérést az oldalt felkereső felhasználónak, de ha az adott felhasználó a kérést elutasította, 6 hónapig nem küldhet újabb hozzájárulás iránti kérést, amikor az adott felhasználó az adott videostreaming oldalról nyújtott videókat tartalmazó más honlapokra látogat.

25. **Pontatlan** továbbá az „online közönség mérésére” vonatkozó kivétel **megfogalmazása**. A javasolt rendelet 8. cikke (1) bekezdésének d) pontja az online közönség mérésére vonatkozó kivételt fogalmaz meg. Az első aggály e téren az, hogy ez a fogalom nincs meghatározva, és összetéveszthető a felhasználókról történő profilalkotással. A fogalommeghatározásnak egyértelművé kell tennie, hogy ez a kivétel nem használható semmilyen profilalkotási célra. A kivétel csak a felhasználó által kért szolgáltatás teljesítésének elemzéséhez szükséges kihasználtsági számításokra vonatkozhat, nem pedig a felhasználók elemzésére (azaz pl. a honlap, alkalmazás vagy eszköz azonosítható felhasználói által tanúsított viselkedés elemzésére). Ez a kivétel ennek megfelelően nem vehető igénybe, amennyiben az adatok összekapcsolhatók a szolgáltató vagy más adatkezelők által feldolgozott, azonosítható felhasználói adatokkal. A kivétel leírása emellett rendkívül technológiaspecifikus felhasználási módot sugall. Az „online közönség mérés” fogalmat ezért újra meg kell határozni úgy, hogy technológiasemleges legyen, és magában foglalja az alkalmazásokból, viselhető eszközökből és a tárgyak internetét alkotó tárgyakból nyert hasonló, a használatra vonatkozó analitikai információkat is.

A munkacsoport azt javasolja, hogy a holland kivétel használják ötletforrásként: ez akkor érvényesíthető, ha a műveletre feltétlenül szükség van az információs társadalommal összefüggő szolgáltatásnyújtás minőségére vagy hatékonyságára vonatkozó információk megszerzéséhez, és nem vagy csak csekély hatással van az érintett (vég)felhasználó magánéletére (lásd a holland távközlési törvény 11.7a cikk (3) bekezdésének b) pontját). Ez a kivétel tekintettel van arra, hogy a weboldalak és alkalmazások elemzése során gyűjtött adatok többsége továbbra is személyes adat. Ez azt jelenti, hogy az ilyen adatok kezelése az általános adatvédelmi rendelet hatálya alá esik. Ebből következik, hogy külső szervezet is végezhet a használatra vonatkozó elemzést, de csak akkor, ha:

- i. a külső szervezet adatfeldolgozóként jár el;
- ii. a felek az általános adatvédelmi rendeletnek megfelelő adatfeldolgozási megállapodást kötnek;
- iii. az alkalmazott elemzési technológia megakadályozza az adatok újraazonosítását, beleértve többek között a felhasználók IP-címének anonimizálását;
- iv. az elemzéshez használt specifikus süti(k) vagy más adatok csak az adott honlaphoz, alkalmazáshoz vagy viselhető eszközhöz használhatók, és nem kapcsolhatók össze más, azonosítható adatokkal;
- v. a felhasználóknak joguk van a részvételt elutasítani (lásd még a vélemény 17. és 50. megjegyzését).

Annak ellenére, hogy e feltételek fennállása esetén nem lenne szükség hozzájárulásra, az adatkezelők továbbra is kötelesek a felhasználókat megfelelően tájékoztatni, például a Do Not Track szabvány nyomkövetési státuszt jelölő mezői révén.¹⁵

26. Az elektronikus hírközlési adatvédelmi rendeletnek **biztosítania kell a hozzájárulásra vonatkozó követelmények alóli kivételek szűk körűségét és pontos megfogalmazását.** A berendezések működésébe történő beavatkozásra vonatkozó hozzájárulás követelménye alóli kivétel 8. cikk (1) bekezdésének c) pontjában rögzített megfogalmazása majdnem megegyezik az elektronikus hírközlési adatvédelmi irányelv 5. cikke (3) bekezdésének jelenlegi szövegezésével: *“amely az előfizető vagy felhasználó által kifejezetten kért, információs társadalommal összefüggő szolgáltatás nyújtásához feltétlenül szükséges”*, azonban a kritikus fontosságú „feltétlenül” szót minden magyarázat nélkül elhagyták belőle. Ez két okból is aggodalomra ad okot. Egyrészt az elektronikus hírközlési adatvédelmi irányelv rendelkezése már így is rengeteg vitához vezetett a felügyeleti hatóságok és a szervezetek között annak hatályáról, és a „feltétlenül” szó elhagyása tovább gyengíti a jogbiztonságot. Ez azért is aggályos, mert a munkacsoport már iránymutatást adott ki a „feltétlenül” szó e szöveggörnyezetben történő értelmezéséről. A munkacsoport az alábbi pontosításra tett javaslatot a sütikre vonatkozó jóváhagyás alóli kivételről szóló véleményében (WP 194):

„A süti feltétlenül szükséges a specifikus funkció felhasználónak (vagy előfizetőnek) történő nyújtásához: a süti letiltása esetén a funkció nem érhető el, és az adott funkciót a felhasználó (vagy előfizető) az információs társadalommal összefüggő valamely szolgáltatás részeként kifejezetten kérte.”¹⁶

A munkacsoport tisztázta továbbá, hogy:

a „harmadik féltől származó” sütik általában nem „feltétlenül szükségesek” az adott honlapot felkereső felhasználó számára, mert ezek a sütik rendszerint a felhasználó által „kifejezetten kért” szolgáltatástól különálló szolgáltatáshoz kapcsolódnak¹⁷.

A munkacsoport hozzátette, hogy a platformot vagy honlapot nem használó személyekre irányuló közösségi beépülők használata ehhez hasonlóan szintén nem tekinthető feltétlenül szükségesnek.

Továbbá, miközben a javasolt rendelet 6. cikke (1) bekezdésének b) pontja lehetővé teszi az elektronikus kommunikációs adatok kezelését akkor, ha az a biztonság érdekében „szükséges”, az általános adatvédelmi rendelet (49) preambulumbekzdése annak feltétlen szükségességét írja elő. Lehetséges, hogy a „feltétlenül” szó elhagyása nem volt szándékos, mivel a javasolt rendelet (21) preambulumbekzdésében az szerepel, hogy a „feltétlenül szükséges” beavatkozáshoz nem kell jóváhagyást kérni.

¹⁵ Lásd: Tracking Preference Expression (DNT), Editor's draft, 2016. március 7.

¹⁶ 29. cikk szerinti munkacsoport, WP 294, 04/2012 sz. vélemény a sütikre vonatkozó jóváhagyás alóli kivételről; elfogadás időpontja: 2012. június 7., url: http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2012/wp194_en.pdf.

¹⁷ Ld. ugyanott.

A javasolt rendelet mindenesetre lehetőség annak további tisztázására, hogy a szükségességet a rendeletben engedélyezett minden kivételesetén szűken kell értelmezni. A munkacsoport ezért javasolja a „feltétlenül” szó beillesztését a „szükséges” elé a javasolt rendelet 6. cikkében és 8. cikkének (1) bekezdésében szereplő minden kivétel esetében.

Az elektronikus hírközlési adatvédelmi rendeletnek ezzel szemben kifejezetten lehetővé kell tenni a beavatkozást, ha annak célja biztonsági frissítés telepítése. A legtöbb végfelhasználói eszköz esetében a biztonsági frissítések telepítésének előnyben részesített módja azok interneten történő kiküldése. A frissítések telepítése a végberendezés működésébe történő beavatkozásnak minősül. Jogos érdek fűződik annak biztosításához, hogy ezeknek az eszközöknek a biztonsági megoldásai folyamatosan frissüljenek. A biztonsági frissítések nyújtóinak általában képesnek kell lenniük a feltétlenül szükséges biztonsági frissítéseket a végfelhasználó jóváhagyása nélkül telepíteni. Nem egyértelmű azonban, hogy erre a beavatkozásra érvényes-e a beavatkozások tilalma alóli, az információs társadalommal összefüggő kivétel (8. cikk (1) bekezdésének c) pontja). Tisztázni kell, hogy ez a kivétel lehetővé teszi a biztonsági frissítések telepítését, de csak akkor, ha i. azok különálló csomagokat képeznek, és semmilyen módon nem módosítják a szoftver működését az adott eszközön (beleértve a más szoftvekkal való interakciót és a felhasználó beállításait), ii. a végfelhasználó minden alkalommal tájékoztatást kap a frissítés telepítése előtt, és iii. a végfelhasználónak lehetősége van kikapcsolni a frissítések automatikus telepítését.

KÖZVETLEN ÜZLETSZERZÉS

Az aggályok egy másik csoportja a közvetlen üzletszerzés elleni védelem elégtelenségére vonatkozik.

27. Az első aggályos pont ezen a téren a **közvetlen üzletszerzés tartalmának túl szűk körű értelmezése**. A javasolt rendelet 4. cikke (3) bekezdése f) pontjának fogalm meghatározása szerint „közvetlen üzletszerzési célú közlés” „minden olyan reklám, akár írásos, akár szóbeli, amelyet az elektronikus hírközlési szolgáltatások egy vagy több azonosított vagy azonosítható végfelhasználójának küldenek”. A „küldenek” szó használata olyan kommunikációs technológia használatát sugallja, amely szükségszerűen a közlés továbbításával jár, a legtöbb webes (közösségi médiában vagy weboldalakon történő) reklám esetében azonban nincs szó a hirdetés szigorúan vett „küldéséről”. Fokozza a problémát a meghatározásban ezt követően felsorolt példák (SMS, e-mail), és a (33) preambulumbekkezdés példái. Ezek mindegyike az üzletszerzési célú kommunikáció meglehetősen hagyományos formáját jelöli, és még így is vitatható, hogy a meghatározás lefedi-e a – teljesen hagyományos – telefonos hívórendszereket. A cikket és a preambulumbekkezdést szükséges lenne úgy módosítani, hogy az egy vagy több azonosított vagy azonosítható végfelhasználónak *küldött, rá irányuló vagy hozzá intézett* valamennyi reklámot magában foglalja. Biztosítani kell továbbá, hogy a magatartás alapú (a végfelhasználók profilján alapuló) reklámozás szintén „egy vagy több azonosított

vagy azonosítható felhasználóra” irányuló, közvetlen üzletszerzési célú közlésnek minősüljön (hiszen az ilyen reklámok konkrét, azonosítható felhasználókat céloznak).

Továbbá a „közvetlen üzletszerzési célú közlés” javasolt meghatározása esetén a 16. cikk (1) bekezdése szerinti védelem a reklámot tartalmazó üzenetekre korlátozódna, és nem védené az egyéneket az üzletszerzési célból nekik küldött, rájuk irányuló vagy hozzájuk intézett egyéb üzenetektől (például a kereskedelmi megkeresésekre vonatkozó jóváhagyást kérő, a politikai nézeteket vagy szavazási preferenciákat népszerűsítő, a jótékonyági és más non-profit szervezeteket népszerűsítő, illetve egy szervezet általános márkáépítését szolgáló üzenetektől). Továbbá a faxberendezéseket is használják még közvetlen üzletszerzés céljára, bár ezeket a meghatározás nem említi. A 4. cikk (3) bekezdése f) pontjának tehát ki kell terjednie a reklámozás, megkeresés és népszerűsítés minden formájára, a non-profit szervezetek esetében is, és az e-mail és SMS mellett kifejezetten meg kell említenie a faxberendezéseket is (lásd még a 43(a) megjegyzés pontosítási javaslatát is). Végezetül a (32) preambulumbekendés rögzíti, hogy a politikai pártok által küldött, a pártot népszerűsítő üzenetek is közvetlen üzletszerzésnek minősülnek. Ezt úgy kellene módosítani, hogy kiterjedjen a politikusokra és azokra a jelöltekre is, akik a megválasztásukért kampányolnak.

28. Második pont: **a közvetlen üzletszerzésre vonatkozó hozzájárulás visszavonása nem díjmentes, és nem is ugyanolyan egyszerű, mint a hozzájárulás megadása.** Az egységesség fokozása és a címzettek védelmének erősítése érdekében pontosítani kell a javasolt rendelet hozzájárulás visszavonására vonatkozó rendelkezését. A javasolt rendelet 16. cikkének (6) bekezdése jelenleg úgy rendelkezik, hogy a közvetlen üzletszerzés címzettjei számára biztosítani kell „azokat az információkat, amelyek szükségesek ahhoz, hogy a címzett egyszerű módon gyakorolhassa a hozzájárulás visszavonásához való jogát a további közvetlen üzletszerzési célú közlések fogadása tekintetében”. Ezt a (34) preambulumbekendés is megerősíti. Az általános adatvédelmi rendelet (70) preambulumbekendéséből azonban az következik, hogy az érintett számára nem csak arra kell biztosítani jogot, hogy egyszerű módon tiltakozzon a közvetlen üzletszerzési célú adatkezelés ellen, de arra is, hogy ezt díjmentesen tegye. Ezt a kifejezést a javasolt rendelet 16. cikkének (2) bekezdése is használja, de csak a vásárlás alkalmával szerzett kapcsolatfelvételi adatokon alapuló közvetlen üzletszerzésben való részvétel elutasítása kapcsán.

Az általános adatvédelmi rendelet 7. cikkének (3) bekezdése előírja, hogy a hozzájárulás visszavonását ugyanolyan egyszerű módon kell lehetővé tenni, mint annak megadását, és hogy a hozzájárulásnak bármikor visszavonhatónak kell lennie. A munkacsoport FEDMA-ról szóló 04/2010. sz. véleménye (WP174) már rögzítette, mennyire fontos „egy egyszerű, hatásos, díjmentes, közvetlen, könnyen hozzáférhető leiratkozási módszer” biztosítása a közvetlen üzletszerzés tekintetében¹⁸. A

¹⁸ 29. cikk szerinti munkacsoport, WP174, 04/2010. sz. vélemény a FEDMA személyes adatok közvetlen üzletszerzés céljából történő felhasználására vonatkozó európai etikai kódexéről; elfogadás időpontja: 2010. július 13., url: http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2010/wp174_en.pdf.

hozzájárulás visszavonása tekintetében ezeket az elvárásokat szükséges beépíteni a javasolt rendelet közvetlen üzletszerzésre vonatkozó szabályaiba. Ugyanez igaz az általános adatvédelmi rendelet 7. cikkének (3) bekezdésében foglalt előírásra, amely szerint a hozzájárulás visszavonását ugyanolyan egyszerű módon kell lehetővé tenni bármikor, mint annak megadását.

29. Ehhez kapcsolódik, hogy **pontosítani kell a közvetlen üzletszerzésre vonatkozó hozzájárulás visszavonásának, illetve az abban való részvétel elutasításának módját.** A javasolt rendelet 16. cikkének (4) bekezdése alapján a tagállamok dönthetnek úgy, hogy a hang alapú, üzletszerzési célú hívások tekintetében a részvétel elutasításának jelzésén alapuló szabályozást alkalmaznak. Az elektronikus hírközlési adatvédelmi rendeletnek meg kell határoznia az üzletszerzési célú hívásokra vonatkozó hozzájárulás visszavonásának, valamint a részvétel elutasításának módját. A (36) preambulumbekkezdés rögzíti, hogy a tagállamoknak *képesnek kell lenniük* a részvétel visszautasítását rögzítő nemzeti rendszerek létrehozására és/vagy fenntartására. E rendelkezés alapján a tagállamok tehát lehetővé tehetik akár egy olyan helyzet előállítását is, amikor a felhasználónak külön-külön kellene jeleznie a részvétel elutasítását az egyes hírközlési szolgáltatók felé. A megvalósítás e formája nem védi a felhasználókat a kéréstlen közlések jelentette zavarástól¹⁹, és nem biztosít az általános adatvédelmi rendeletnek megfelelő mechanizmust a hozzájárulás egyszerű módon, bármikor történő visszavonására sem. A rendeletnek ezért azt kell előírnia, hogy minden tagállam *köteles* létrehozni egy nemzeti „Ne hívj” nyilvántartást. A rendeletnek azt is rögzítenie kell, hogy a hang alapú hívások címzettjeinek kétféle lehetőséget kell biztosítani a hozzájárulásuk visszavonására: az adott vállalat vagy szervezet további hívásaira vonatkozóan, illetve a hívás során lehetőséget kell biztosítani számukra a nemzeti „Ne hívj” nyilvántartásba történő bejelentkezésre.
30. Aggályos továbbá a **hamis azonosító adatok használatára vonatkozó kifejezett tiltás hiánya a közvetlen üzletszerzési célú közlések során.** A (34) preambulumbekkezdés megjegyzi, hogy „a közvetlen üzletszerzést célzó, kéréstlen kereskedelmi közlések küldése során tilos „a küldő kilétének elfedése, valamint a hamis azonosító adatok, hamis válaszcím vagy hamis választ telefonszám alkalmazása”. A 16. cikk (4) bekezdése azonban csak azt írja elő, hogy a végfelhasználókat tájékoztatni kell „annak a jogi vagy természetes személynek a kilétéről, aki/amely megbízásából a közlést továbbítja”. A címzettek megbízó kilétéről való tájékoztatásának kötelezettségét ki kell egészíteni a rejtett vagy hamis kapcsolattartási címek használatára vonatkozó egyértelmű tiltással a közvetlen üzletszerzés terén.
31. Ez a probléma egy másik aggályos ponthoz is kapcsolódik: **a közvetlen üzletszerzési hívások esetében az előhívószám alkalmazásának követelménye a kapcsolattartási vonal azonosítására vonatkozó követelmény alternatívájaként jelenik meg.** A 16. cikk (3) bekezdése értelmében a közvetlen üzletszerzési célú

¹⁹ Az Egyesült Királyságban például a BT távközlési vállalat egyetlen hét alatt 31 millió kéréstlen hívást rögzített. Lásd: <http://www.bbc.com/news/business-38635921>.

hívás akkor megengedett, ha i. megnevez egy olyan vonalat, amelyen a hívó természetes vagy jogi személy elérhető (16. cikk (3) bekezdésének a) pontja, vagy ii. meghatározott kódot/előhívószámot alkalmaz, amely a hívást üzletszerzési célú hívásként azonosítja (16. cikk (3) bekezdésének b) pontja). Míg a munkacsoport üdvözli a 16. cikk (3) bekezdésének b) pontjában foglalt, az előhívószám alkalmazására vonatkozó előírást, véleménye szerint ez a követelmény nem ugyanazon kérdés kezelését szolgálja, mint a 16. cikk (3) bekezdése a) pontjában előírt, a kapcsolattartásra alkalmas vonal megnevezésére vonatkozó követelmény. Az előhívószámra vonatkozó követelmény célja ugyanis, hogy a címzett már előre üzletszerzési célú hívásként azonosíthassa a hívást (és alkalmazhasson az ilyen hívások kiszűrésére vonatkozó intézkedéseket), míg a kapcsolattartásra alkalmas vonal megnevezésére vonatkozó követelmény célja, hogy a címzetek (és a felügyeleti hatóságok) azonosíthassák azt, aki az üzletszerzésre megbízást adott, és felvehessék vele a kapcsolatot. Ez különösen fontos az automatikus hívások esetében, ahol jelentős egyensúlyhiány áll fenn az üzletszerzést végző fél kéretlen hívások kiküldésére való képessége és a címzetek ilyen hívások elkerülésére vonatkozó lehetőségei között. Ezeknek a követelményeknek nem egymás alternatíváinak, hanem egymást kiegészítő követelményeknek kell lenniük.

MENETREND

32. A 29. cikk szerinti munkacsoport dicséretesnek tartja, hogy az Európai Bizottság szerint a javasolt rendeletnek 2018 májusában, az általános adatvédelmi rendelettel azonos időben kell hatályba lépnie, elkerülendő a két jogalkotási aktus közötti ellentmondásokat. Aggodalomra ad okot azonban az, hogy ez az időzítés tekintetében nagyratörő cél, amihez a még tervezet formában lévő Európai Elektronikus Hírközlési Kódexet is véglegesíteni kell. A munkacsoport ezért azt kéri, hogy a jogalkotási folyamatban részt vevő minden érdekelt kötelezze el magát a 2018. májusi határidő mellett.

TOVÁBBI AGGÁLYOK

Ez a fejezet további, aggodalomra okot adó kérdések ismertetését tartalmazza.

33. A munkacsoport aggályosnak találja először is annak **sugalmazását, hogy a nem célzott adatmegőrzési intézkedések elfogadhatóak**. Az indoklásban szerepel, hogy a javasolt rendelet továbbra is lehetővé teszi a tagállamok számára olyan nemzeti adatmegőrzési szabályrendszer fenntartását vagy létrehozását, amely többek között célzott adatmegőrzési intézkedéseket tesz lehetővé (1.3 pont). A *Tele2/Watson*-határozatot²⁰ követően egyértelmű, hogy a Charta értelmében nem megengedettek az olyan adatmegőrzési szabályrendszerek, amelyek a célzott adatmegőrzésen kívül más is lehetővé tesznek (és még azoknak is olyan fontos feltételeknek kell megfelelniük, mint például a felügyelet), és hogy a metaadatokhoz való általános jellegű hozzáférést

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

ugyanúgy a 7. cikkbe ütközőnek kell tekinteni, mint az elektronikus közlések tartalmához való általános jellegű hozzáférést (ld. EUB, Schrems, és (94) preambulumbekzdés). Ennek a mondatnak a megfogalmazása tehát azt sugallja, hogy a tagállamoknak olyan mozgástere van az adatmegörzési intézkedések terén, amellyel valójában nem rendelkeznek. Ehhez kapcsolódik, hogy a javasolt rendelet **nem biztosít megfelelő szintű védelmet a metaadatok számára**. Amint a 10. megjegyzés rámutat, a 29. cikk szerinti munkacsoport üdvözlí annak felismerését, hogy a metaadatok nagyon érzékeny adatokat fedhetnek fel. A javasolt rendelet azonban nem biztosít az e felismerésből következónak megfelelő szintű védelmet a metaadatok számára. A metaadatok érzékeny jellegére való tekintettel különösen a 6. cikk (2) bekezdésének c) pontja szerinti elemzés előtt – adatvédelmi hatáselemzést kellene végezni (lásd a 46. megjegyzést is).

34. Másodszor, **a javasolt rendelet nemkívánatos mértékben kiszélesítené az adatok megörzésének lehetőségét**. A javasolt rendelet 11. cikke az általános adatvédelmi rendelet 23. cikke (1) bekezdésének a)-e) pontjára hivatkozva ismerteti azokat a célokat, amelyek érdekében a tagállamok korlátozhatják a rendelet 5-8. cikkében rögzített kötelezettségeket és jogokat. Az általános adatvédelmi rendelet az érintettek számára jelentett magas kockázatra való tekintettel nem tesz lehetővé ilyen korlátozást a speciális kategóriába tartozó adatok tekintetében. Az elektronikus hírközlési adatvédelmi irányelv 15. cikke jelenleg engedélyez hasonló korlátozást, de csak korlátozottabb célokból. Az új, javasolt rendelet új korlátozásokat tenne lehetővé a „büntetőjogi szankciók végrehajtása, beleértve a közbiztonságot fenyegető veszélyekkel szembeni védelmet és e veszélyek megelőzését” céljából (általános adatvédelmi rendelet 23. cikke (1) bekezdésének d) pontja) és az „Unió vagy valamely tagállam egyéb fontos, általános közérdekű célkitüzései, különösen az Unió vagy valamely tagállam fontos gazdasági vagy pénzügyi érdeke, beleértve a monetáris, a költségvetési és az adózási kérdéseket, a népegészségügyet és a szociális biztonságot” céljából (általános adatvédelmi rendelet 23. cikke (1) bekezdésének e) pont). Azon túl, hogy ezek a célok az elektronikus hírközlési adatvédelmi irányelvben szereplőkhöz képest újak, a 23. cikk (1) bekezdésének d) pontjában foglalt utolsó cél, valamint a 23. cikk (1) bekezdésének e) pontjában foglalt cél egésze rendkívül tágan van megfogalmazva. Ezért javasoljuk az általános adatvédelmi rendelet 23. cikke (1) bekezdésének a)-e) pontjaira vonatkozó hivatkozás törlését, és csak a jelenleg az elektronikus hírközlési adatvédelmi irányelv 15. cikkében szereplő célok szerepeltetését.

35. **A felhasználók biztonsági kockázatokról való tájékoztatására vonatkozó kötelezettség a minimumra szorítkozóan van megfogalmazva**. A munkacsoport üdvözlí, hogy a szolgáltatóknak tájékoztatniuk kell a felhasználókat a biztonsági kockázatokról és az ezek kezelésére alkalmazott intézkedésekről, mint például a titkosítás (17. cikk és (37) preambulumbekzdés). A rendelkezés címe azonban ez: „Értesítés az észlelt biztonsági kockázatokról”. Az, hogy a címben az „észlelt kockázatok” kifejezés szerepel, azt sugallja, hogy ez a rendelkezés csak a (potenciális) biztonsági incidensekre vonatkozik, miközben a rendelkezés és a preambulumbekzdés megfogalmazása inkább a végfelhasználók általános felvilágosítására utal. Ha például a szolgáltató észleli, hogy egy felhasználó eszköze káros programmal fertőzött meg, és egy bothálózat része lett, úgy tűnik, hogy ez a

rendelkezés közvetlenül kötelezi a szolgáltatót arra a felhasználó értesítésére az ebből eredő kockázatokról. A rendelkezés tartalma azonban pontosítható lenne, és nem korlátozódhat erre az egy helyzetre. A rendelkezésnek ki kell terjednie legalább a szolgáltató által az előfizetés részeként a végfelhasználónak biztosított valamennyi eszközben (pl. útválasztók, mobil eszközök) észlelt biztonsági kockázatokra, továbbá a beépített adatvédelem elvének megfelelő, a magánéletet védő beállítások módosításával járó kockázatokról szóló tájékoztatásra.

A munkacsoport javasolja a rendelkezés kiterjesztését az elektronikus kommunikációt lehetővé tévő szoftverek nyújtóira (lásd a (8) preambulumbekendést), és esetleg egy új kategóriára is: a kommunikáció biztonságához elengedhetetlen technológiát nyújtó, szolgáltatónak nem minősülő felekre (pl. titkosítási technológiák nyújtóira). A rendelkezés hatályának utóbbiak szerinti kiterjesztése esetén ügyelni kell arra, hogy ne legyen átfedés e kötelezettség és a biztonsági incidensek bejelentésére vonatkozóan más jogalkotási aktusokban, például a hálózati és információs rendszerek biztonságáról szóló irányelvben²¹ vagy más, a tanúsítványszolgáltatókra vonatkozó jogi instrumentumokban előírt kötelezettségek között. Miután az utóbbi kategóriába tartozó technológiaszolgáltatók általában nem állnak közvetlen kapcsolatban a végfelhasználókkal, azt is rögzíteni kell, hogyan tehetnek eleget az e rendelkezésből eredő kötelezettségüknek.

36. A munkacsoport üdvözli a 2. és 13. cikk számfüggő személyközi kommunikációs szolgáltatásokra vonatkozó rendelkezéseit. Nem nyilvánvaló azonban, miért **nem szükséges a magánélet ugyanilyen szintű védelmét biztosítani a funkcionálisan ezzel egyenértékű hálózatsemleges hívási szolgáltatások tekintetében.**
37. A munkacsoport aggasztónak tartja továbbá a **névjegyzékekben végzett visszakereséshez való többszintű hozzájárulás nem kellően egyértelmű szabályozását.** A javasolt rendelet 15. cikkének (2) bekezdése értelmében a szolgáltatónak a végfelhasználó hozzájárulását kell kérnie az adatokkal kapcsolatos keresési funkciók aktiválása előtt (lásd a (31) preambulumbekendést is). A munkacsoport üdvözli a névjegyzékekben történő szerepeltetésre vonatkozó hozzájárulási követelmények harmonizálását, de sajnálja, hogy hiányzik a lehetőség az eltérő típusú keresésekre vonatkozóan eltérő hozzájárulások megadására. A jelenlegi elektronikus hírközlési adatvédelmi irányelv lehetővé teszi a tagállamok számára, hogy a 12. cikk (3) bekezdése alapján külön jóváhagyási követelményt írjanak elő a visszakereséshez. Az említett cikk értelmében: „*A tagállamok előírhatják, hogy a személyek elérhetőségi adatainak név és szükség esetén más minimális azonosító adat alapján történő keresését kivéve, a nyilvános előfizetői névjegyzék bármilyen más célból történő felhasználásához az előfizetők kiegészítő hozzájárulására legyen szükség*”. Számos tagállam e rendelkezés alapján külön hozzájárulást ír elő az ellenirányú keresési funkciókhoz, figyelembe véve az

²¹ Az Európai Parlament és a Tanács (EU) 2016/1148 irányelve (2016. július 6.) a hálózati és információs rendszerek biztonságának az egész Unióban egységesen magas szintjét biztosító intézkedésekről (HL L 194., 2016.7.19., 1-30. o.), url: <http://eur-lex.europa.eu/legal-content/HU/TXT/HTML/?uri=CELEX:32016L1148&from=HU>

azonosíthatóság eltérő szintjeit és ezzel a kétféle funkció jelentette beavatkozás eltérő mértékét.

38. Formálisabb probléma, hogy **a bírságok mértéke a rendelet megsértésének nem minden esetére vonatkozóan harmonizált.** A javasolt rendelet rögzíti, hogy a tagállamok meghatározzák a javasolt rendelet 23. cikkének (4) bekezdése, 23. cikkének (6) bekezdése és 24. cikke megsértéséért járó szankciók mértékét. Egységesebb lenne ezt magában az elektronikus hírközlési adatvédelmi rendeletben is szabályozni.
39. Végezetül, **a javasolt rendelet olyan fogalommeghatározásokra támaszkodik, amelyek változhatnak.** A javasolt rendelet a kulcsfogalmak egy része tekintetében egy másik, még csak tervezet formájában létező jogi aktusra hivatkozik: a javasolt Európai Elektronikus Hírközlési Kódexre (lásd például: 4. cikk (1) bekezdésének b) pontja). Ennek két fontos példája a „végfelhasználó” meghatározása, amely jelenleg a természetes és a jogi személyeket is magában foglalja, valamint az „elektronikus hírközlési szolgáltatás” és a „személyközi kommunikációs szolgáltatás” meghatározása, amelyet jelenleg a javasolt rendelet 4. cikke (1) bekezdésének b) pontja tükröz, illetve a második esetében a 4. cikk (2) bekezdése tovább részletez oly módon, hogy az Európai Elektronikus Hírközlési Kódex által kifejezetten kizárt típusú szolgáltatásokat is magában foglalja.²² Ez a vélemény a fogalommeghatározások jelenlegi formáját veszi alapul, azonban valószínű, hogy a javasolt Európai Elektronikus Hírközlési Kódex és/vagy annak alapvető fogalmai még módosulnak. Ez pedig azonnali következményekkel járna az elektronikus hírközlési adatvédelmi rendeletre nézve is. Ideális esetben az Európai Elektronikus Hírközlési Kódexből eredő valamennyi kifejezést önállóan definiálni kellene az elektronikus hírközlési adatvédelmi rendeletben, de legalábbis a javasolt rendeletben tisztázni kellene minden olyan esetet, amikor egy adott kifejezés meghatározása eltér az Európai Elektronikus Hírközlési Kódexben szereplő meghatározástól (mint pl. az a fent említett eltérés, hogy a „személyközi kommunikációs szolgáltatások” definíciója a „kiegészítő szolgáltatásokat” is magában foglalja). Ha azonban erre nincs mód, a munkacsoport a jogalkotási folyamatban részt vevő minden fél számára javasolná annak biztosítását, hogy a javasolt rendeletről és az Európai Elektronikus Hírközlési Kódexről szóló vitára, illetve szavazásra azonos időben kerüljön sor, hogy az érdekeltek helyes képet alkothassanak az új jogi aktusok hatályáról és következményeiről.

5. A JOGBIZTONSÁGOT SZOLGÁLÓ PONTOSÍTÁSI JAVASLATOK

A fent ismertetetteken túl a munkacsoport szeretné felhívni a figyelmet a javasolt rendelet egyes rendelkezéseire, amelyek pontosításra szorulnak. Ezeket a pontosításokat

²² A javasolt rendelet 4. cikkének (2) bekezdése például úgy szól, hogy a személyközi kommunikációs szolgáltatás „magában foglalja az olyan szolgáltatásokat is, amelyek csupán egy másik szolgáltatáshoz szorosan kapcsolódó, jelentéktelen járulékos funkcióként teszik lehetővé a személyközi, interaktív kommunikációt”, míg az Kódex 2. cikkének (5) bekezdése kifejezetten kizárja az ilyen szolgáltatásokat a kifejezés meghatározásából. (A Kódex 2. cikk (4) bekezdése a „személyközi kommunikációs szolgáltatásokat” az „elektronikus hírközlési szolgáltatások” szélesebb kategóriáján belül helyezi el.)

szükségesnek tartjuk a jogbiztonság fokozásához minden érdekelt számára, valamint az elektronikus hírközlési adatvédelmi rendelet egységesség értelmezéséhez és alkalmazásához az Unió teljes területén.

A RENDELET HATÁLYÁRA VONATKOZÓ PONTOSÍTÁSOK

40. A munkacsoport a következő javaslatokat teszi a javasolt rendelet hatályának pontosítására:

- a. **A „végfelhasználó” kifejezés foglaljon magában minden egyéni felhasználót.** Az Európai Elektronikus Hírközlési Kódex 2. cikk (14) bekezdésének meghatározása szerint a végfelhasználó olyan felhasználó, aki nem szolgáltató nyilvános hírközlő hálózatokat vagy nyilvánosan elérhető/hozzáférhető elektronikus hírközlési szolgáltatásokat. Tisztázni kell, hogy a javasolt rendelet hatálya alól nincsenek kizárva azok a személyek, akik – például wifi-útválasztójuk kapacitásának rendelkezésre bocsátásával – hozzájárulnak a hálózatok működéséhez.
- b. **Tisztázni kell, hogy a rendelet területi hatálya minden végfelhasználóra kiterjed, aki az Unióban tartózkodik.** A javasolt rendelet 3. cikke (1) bekezdésének a) pontja az elektronikus hírközlési szolgáltatások végfelhasználóknak történő nyújtására vonatkozik „az Unióban”, míg a 3. cikk (1) bekezdésének c) pontja úgy szól, hogy a rendelet az „Unióban található” végfelhasználók végberendezéseinek védelmére vonatkozik (utólagos kiemelés). Ez a különböző fordításokban eltérően jelenik meg. A német fordítás nem tartalmazza ezt a különbséget, míg mások, így a francia, a spanyol és a holland fordítás, tartalmazza. A (9) preambulumbekszegésből egyértelmű, hogy a területi hatályt tágan kívánták meghatározni, tekintet nélkül arra, hogy a szolgáltatásokat az Unión kívülről nyújtják-e, vagy hogy az adatkezelés az Unióban történik-e. Ezért javasoljuk a 3. cikk (1) bekezdésének c) pontjában lévő „található” szó eltávolítását, hangsúlyozandó a rendelet széles területi hatályát.
- c. **Úgy tűnik, mintha a javasolt rendelet a bizalmas közlést csak a továbbítás során védené, a tárolás során nem.** A javasolt rendelet jelenleg a közlések továbbításának védelmére összpontosít. Lásd például a (15) preambulumbekszegést, amely kimondja, hogy a kommunikációs adatok lehallgatásának tilalma azok továbbításának során érvényes, azaz addig, amíg a címzett meg nem kapta a közlésben foglaltakat. A védelem e megfogalmazása a kommunikáció fogalmának olyan felfogásán alapul, amely már elavult. A kommunikációs adatok többsége jelenleg már a kézbesítést követően is a kiszolgálón marad. Biztosítani kell, hogy a védelem ezeknek az adatoknak a titkosságára is vonatkozik. Emellett az ugyanazon felhőalapú szolgáltatás (például web alapú levelezés) előfizetői között zajló kommunikáció során gyakran alig kerül sor „továbbításra”: egy e-mail elküldése leginkább azt jelenti, hogy ennek tükröződnie kell a szolgáltató adatbázisában, nem azt, hogy tényleges üzenetküldésre kerül sor a két fél között. Az az érv, hogy ezt az általános adatvédelmi rendelet már lefedi, nem meggyőző: a javasolt rendelet célja éppen az, hogy minden bizalmas közlést

védjen, tekintet nélkül a közlést megvalósító műszaki megoldásra. Elképzelhető, hogy ez csak szövegezési hiba, mivel az 5. cikkben foglalt tilalom „tárolásra” és „kezelésre” vonatkozik.

- d. **Minden nyilvános vezeték nélküli internet-hozzáférési pontnak a rendelet hatálya alá kell tartoznia.** Tekintettel a vezeték nélküli internet-hozzáférési pontok elterjedt használatára, logikus, hogy nem maradhat kétség afelől, hogy a védelem az ilyen hozzáférési pontokon keresztül továbbított közlések titkosságára is kiterjed. A rendelet ennek tisztázására tett kísérlete azonban sikertelen, mivel annak hatályát csak a „végfelhasználók nem meghatározott csoportja” számára nyújtott hálózatokra terjeszti ki ((13) preambulumbekkezdés). Szükséges lenne a „végfelhasználók nem meghatározott csoportja” és a „végfelhasználók zárt csoportja” kifejezések definiálása. Tisztázni kellene különösen azt, hogy a biztonságos (azaz jelszóval védett) vezeték nélküli hálózatok is a rendelet hatálya alá tartoznak, ha a jelszót a felhasználók elméletileg végtelen csoportja számára biztosítják, akiknek kiléte előre nem határozható meg (például egy kávézó vendégei vagy egy repülőtér látogatói). E téren az alapelv az, hogy a munkacsoportnak az elektronikus hírközlési adatvédelmi irányelv értékelésére vonatkozó korábbi véleményével összhangban *„a hírközlési adatvédelmi aktus alól csak a hivatalos vagy munkaviszonnyal összefüggő szituációban, kizárólag a munkához kapcsolódó, vagy hivatalos célból nyújtott szolgáltatások; a közszférabeli vagy nem közszférabeli szervezetek közötti, kizárólag a munka- vagy üzleti folyamatok szabályozása céljából megvalósuló technikai kommunikáció; valamint a szolgáltatások kizárólag otthoni célra történő igénybe vétele mentesülhet”*. (8. o.)
- e. **A javasolt rendeletek ki kell terjednie a digitális műsorszórási szolgáltatások felkínálása során gyűjtött adatokra is.** Tekintettel a nézői szokások érzékeny, a nézők személyes érdeklődését és tulajdonságait felfedő jellegére, az elektronikus hírközlési adatvédelmi rendeletben (esetleg egy preambulumbekkezdés útján) rögzíteni kell, hogy az elektronikus hírközlési hálózatok segítségével továbbított tartalmakat nyújtó szolgáltatásoknak az elektronikus hírközlési szolgáltatások meghatározásából történő kizárása nem jelenti azt, hogy azok a szolgáltatók, amelyek elektronikus hírközlési szolgáltatásokat és tartalmakat egyaránt kínálnak, ne tartoznának az elektronikus hírközlési adatvédelmi rendelet elektronikus hírközlési szolgáltatások nyújtóira irányuló rendelkezéseinek hatálya alá. Ez különösen fontos azért, mert a javasolt Európai Elektronikus Hírközlési Kódex (2. cikk (4) bekezdése) „elektronikus hírközlési szolgáltatásra” vonatkozó fogalommeghatározása nem foglalja magában a „az elektronikus hírközlő hálózatok segítségével történő tartalomszolgáltatást” nyújtó szolgáltatásokat.
- f. **A kommunikációs adatok általában személyes adatok.** A (4) preambulumbekkezdés rögzíti, hogy a kommunikációs adatok személyes adatokat tartalmazhatnak. Ezzel szemben a kommunikációs adatok többsége

személyes adat,²³ mégpedig nagyrészt igen érzékeny, magánjellegű adat, ezért ezt a kijelentést módosítani kell arra, hogy a kommunikációs adatok rendszerint személyes adatok.

- g. **Az azonos platformon belüli üzenetek is bizalmas közlésnek minősülnek**
Az (1) preambulumbekkezdés rögzíti, hogy a titkosság elve a „jelenlegi és jövőbeni kommunikációs eszközökre” vonatkozik. A preambulumbekkezdés az ilyen eszközök példálózó felsorolásával folytatódik, köztük a „közösségi média segítségével nyújtott személyes üzenetküldéssel”. Ennek célja valószínűleg az, hogy a közösségi hálózatok (pl. Facebook, Twitter) felhasználói közötti magánüzeneteket, vagy az idővonalon közzétett, véges számú személy számára elérhető üzeneteket is lefedje, de a megfogalmazás nem kellően egyértelmű.

- h. **Mennyiben vonatkozik az elektronikus hírközlési adatvédelmi rendelet a gépek közötti interakciókra?** Amint a 9. bekezdésben áll, a munkacsoport üdvözli a védelem kiterjesztését a gépek közötti interakciókra. Ez azonban csak a (12) preambulumbekkezdésben szerepel, a kapcsolódó cikkben nem. Ezen interakciók védelme kívánatos, mivel az ilyen kommunikáció gyakran tartalmaz a magánélet védelméhez való jog által védett információkat. Másfelől viszont a tisztán gépek közötti kommunikáció egy szűk kategóriáját ki kell vonni a rendelet hatálya alól, ha nincs hatással sem a magánéletre, sem a közlés bizalmaságára, mint például azokban az esetekben, amikor a kommunikációra a hálózat elemei (pl. kiszolgálók, kapcsolók) közötti jelátviteli protokoll végrehajtása során kerül sor azzal a céllal, hogy tájékoztassák egymást aktivitási státuszukról.

Egy másik terület, amely kapcsán az elektronikus hírközlési adatvédelmi rendelet alkalmazása különösen pontosításra szorul, az intelligens közlekedési rendszerek kérdése. Az elképzelések szerint a járművek rádióan keresztül folyamatosan sugározni fognak adatokat, köztük egy egyedi azonosítót. Ha az elektronikus hírközlési adatvédelmi rendelet nem biztosít kiegészítő védelmet a kommunikációs adatok számára, ez a vezetési szokások, az útvonalak és a járművezetők sebességének folyamatos nyomon követését eredményezheti. Az Európai Elektronikus Hírközlési Kódex 2. cikkének (1) bekezdése azonban új, kibővített meghatározást kínál a hírközlő hálózatokra vonatkozóan. Ez magában foglalja a központosított adminisztrációs kapacitással nem rendelkező, valamint a rádióhullám útján történő jelátvitelt lehetővé tévő átviteli rendszereket is. Az elektronikus hírközlési adatvédelmi rendelet (14) preambulumbekkezdése rögzíti, hogy az ilyen adatok elektronikus kommunikációs adatok. A javasolt rendelet 5. cikke alapján e kommunikációs adatok bármilyen lehallgatása, megfigyelése vagy tárolása tilos, kivéve, ha valamely meghatározott kivétel fennáll. Érdekünk

²³ Lásd például: az EUB C-101/01. sz. ügyben 2003. november 6-án hozott ítéletének 24. pontját (egy telefonszám tekintetében); az EUB C-582/14. sz. (*Breyer*) ügyben hozott 2016. október 19-én hozott ítéletének, 49. pontját (a dinamikus IP-címek tekintetében); és az EUB C-239/12. és C-594/12. sz. (*Digital Rights Ireland*) ügyben 2014. április 8-án hozott ítéletének 26-27. pontját (a metaadatok érzékenysége tekintetében).

fűződik azonban ezen adatok kezeléséhez abból a célból, hogy az önvezető autók és más hasonló berendezések figyelmeztethessék egymást a közelségükre vagy más kockázatokra. A kérdés az, hogy melyik kivétel alkalmazható erre az esetre. A végfelhasználóktól kapott jóváhagyás nem alkalmas kivétel, mert szükség lehet arra, hogy folyamatosan mód nyíljon az adatok kezelésére. A szolgáltatóknak ezért konkrét kivételre kell tudniuk támaszkodni, amely lehetővé teszi az önvezető autók és más hasonló berendezések számára, hogy figyelmeztessék egymást a közelségükre vagy más kockázatokra.

A JÓVÁHAGYÁS FOGALMÁNAK ÉS ALKALMAZÁSÁNAK PONTOSÍTÁSA

41. A munkacsoport az alábbi javaslatokat teszi a jóváhagyás fogalmának és alkalmazásának a jelen javasolt rendeletben történő pontosítására:

- a. **A jóváhagyás alkalmazása jogi személyek tekintetében.** A (3) preambulumbekzdés értelmében a rendeletnek biztosítania kell, hogy az általános adatvédelmi rendelet rendelkezései a jogi személyiséggel rendelkező végfelhasználókra is vonatkozzanak. A preambulumbekzdés értelmében ez magában foglalja a jóváhagyás általános adatvédelmi rendelet szerinti meghatározását (lásd a (18) preambulumbekzdést is). Amint a 13. megjegyzésben jeleztük, a munkacsoport üdvözli, hogy a rendelet hatálya kifejezetten kiterjed a jogi személyekre. Ennek az elvnek a gyakorlati alkalmazása azonban nem egyértelmű. A jóváhagyás általános adatvédelmi rendeletben foglalt meghatározása értelmében a jóváhagyásnak „megfelelő tájékoztatáson alapulónak” kell lennie, és az érintett akaratát „nyilatkozat vagy a megerősítést félreérthetetlenül kifejező cselekedet útján” kell kinyilvánítani (általános adatvédelmi rendelet 4. cikkének (11) bekezdése). Tisztázni kell, hogy mikor tekinthető egy jogi személy „megfelelő tájékoztatás” birtokában lévőnek, és mi minősül a jogi személy akaratának fentiek szerinti kinyilvánításának.
- b. Ezzel kapcsolatban érdemes megjegyezni, hogy a munkáltató a legtöbb helyzetben nem adhat hozzájárulást a munkavállalói nevében, mivel a munkáltató által a munkavállalóhoz intézett, jóváhagyásra vonatkozó kérés esetén az egyenlőtlen erőviszonyokra való tekintettel a hozzájárulás megtagadásából valós vagy potenciális, releváns hátrány származhat, ezért az ilyen jóváhagyás nem önkéntes, így nem érvényes²⁴. **A javasolt rendelet nem tartalmaz (megfelelő) kivételt a beavatkozás tilalma alól a vállalatok által az egyes személyeknek kiadott eszközök és berendezések tekintetében.** Példa erre az az eset, amikor a munkáltató frissíteni szeretné a vállalat által biztosított telefont. Egy másik példa, amikor a munkáltató bérelhető autót kínál a munkavállalók számára, és egy harmadik fél számára engedélyezi, hogy az adminisztrációs feladatok elvégzéséhez a tartózkodási

²⁴ Lásd a jóváhagyás meghatározásáról szóló 15/2011 sz. véleményt (WP 187), a személyes adatok munkaviszonnyal összefüggő kezeléséről szóló 8/2001. sz. véleményt (WP48), és a munkahelyi adatkezelésről szóló új (ezzel a véleménnyel azonos időben elfogadott) véleményt.

helyre vonatkozó adatokat gyűjtsön a jármű fedélzeti egységéből. A munkáltatónak mindkét esetben érdeke fűződik az említett berendezések működésébe való beavatkozáshoz.

Ez a beavatkozás nem tekinthető valamely információs társadalommal összefüggő szolgáltatás nyújtásához (8. cikk (1) bekezdésének c) pontja), sem az „online közönség méréséhez” (8. cikk (1) bekezdésének d) pontja). A megoldás egy új kivétel létrehozása lenne, amely magában foglalja azokat a helyzeteket, amikor i. a munkáltató bizonyos berendezéseket bocsát rendelkezésre a munkaviszonnyal összefüggésben, ii. az említett berendezés felhasználója a munkavállaló, és iii. a beavatkozás feltétlenül szükséges a berendezés munkavállaló általi működtetéséhez (feltételezve az arányosság és a szubszidiaritás elvének betartását az adatgyűjtés terén). A munkáltató csak akkor avatkozhat be a végfelhasználó berendezésének működésébe, ha mindezen feltételek teljesülnek.

- c. **Az automatikus hívástovábbítás kiküszöbölésére szolgáló eszközök tökéletesítése.** A 14. cikk fontos eszközt biztosít a végfelhasználók számára a harmadik felek általi automatikus hívástovábbítás kiküszöböléséhez. Ez a védelem továbbfejleszthető azzal, ha a végfelhasználó hozzájárulása már a hívástovábbítás kezdeményezésének is feltétele.

TARTÓZKODÁSI HELYRE VONATKOZÓ ADATOKKAL ÉS MÁS METAADATOKKAL KAPCSOLATOS PONTOSÍTÁSOK

42. A munkacsoport az alábbi pontosításokra tesz javaslatot a tartózkodási helyre vonatkozó adatok és más metaadatok tekintetében:

- a. **A (17) preambulumbekkezdésben a „nem elektronikus hírközlési szolgáltatások nyújtásával összefüggésben létrejött, tartózkodási helyre vonatkozó adatok”** kifejezés jelentése pontosításra szorul. Nem egyértelmű, hogy ez például az okoseszközök GPS-funkciójából származó adatokat felhasználó és/vagy a közeli wifi-útválasztókon alapuló, tartózkodási helyre vonatkozó adatokat létrehozó alkalmazásokból gyűjtött, és/vagy a navigációt segítő fedélzeti rendszerekből gyűjtött, tartózkodási helyre vonatkozó adatokra, esetleg a tartózkodási helyre vonatkozó adatok létrehozásának egyéb módjaira vonatkozik-e. Az egyértelműség hiánya jogbizonytalanságot teremt a kötelezettség tartalma tekintetében. A természetes személyek végberendezéseinek tartózkodási helyre vonatkozó adatai mindenesetre mindig személyes adatok, ezért ezek kezelésére az általános adatvédelmi rendeletben foglalt kötelezettségek vonatkoznak.
- b. Tisztázni kell, hogy a **tartózkodási helyre vonatkozó adatok és más metaadatok jogszerű kezeléséhez a legtöbb esetben nincs szükség egyedi azonosítóra.** A (17) preambulumbekkezdés a hőtérképeket említi az elektronikus kommunikációs metaadatoknak az elektronikus hírközlési szolgáltatások nyújtói általi, kereskedelmi célú felhasználásának példjaként. Egy alapszintű hőtérkép létrehozásához azonban nincs szükség egyedi azonosítóra, a statisztikai számlálás elegendő. A preambulumbekkezdésben említett másik példa, az infrastruktúra kihasználtsága és leterheltsége szintén meghatározható bizonyos mérési pontok segítségével, például a

forgalomirányító tornyok használatára vonatkozó összesített kimutatások készítésével, amelyekből megismerhető a leterheltség mértéke egy adott ponton és időpontban, anélkül, hogy a toronyhoz kapcsolódó személyek személyazonosságának ismeretére is szükség lenne.

A preambulumbekzdés példaként említi továbbá a meghatározott időszakban végbemenő, meghatározott irányú forgalom megjelenítését, aminél szükség van egyedi azonosítóra ahhoz, hogy az egyének meghatározott időközönként vizsgált tartózkodási helye összekapcsolható legyen. Úgy tűnik, mintha a preambulumbekzdés ezzel legitimálná az ilyen adatok „big data” adatelemzés céljára történő további kezelését. A javasolt rendelet az ilyen adatkezelés tekintetében egyetlen feltételt támaszt: az adatvédelmi hatásvizsgálat elvégzésének kötelezettségét abban az esetben, ha az adatfeldolgozás *várhatóan nagy kockázatot jelent a természetes személyek jogaira és szabadságaira nézve*. Ez a feltétel nem elégséges. Ezenfelül ellentétes azzal a 6. cikkben foglalt kötelezettséggel, hogy ilyen adatkezelés csak a felhasználók jóváhagyásával végezhető, és csak akkor, ha az adatok nem anonimizálhatók, azaz az egyedi azonosítók nem mellőzhetők. A felhasználók sokszor nem utasíthatják vissza a földrajzi helyzetükre vonatkozó adatok elektronikus hírközlési szolgáltatást nyújtók általi gyűjtését, mert az adatgyűjtés műszakilag szükséges ahhoz, hogy a közléseket eljuttathassák a felhasználóhoz, vagy mert az adatkezelés szükséges a kért (például navigációs) szolgáltatás nyújtásához. Korábbi véleményeiben a munkacsoport megállapította, hogy az ilyen jellegű, okos eszközökről származó, tartózkodási helyre vonatkozó adatok érzékeny személyes adatok, és hogy az ezek elemzéséből származó előnyök nem élveznek előnyt a felhasználók kommunikációs metaadataik titkosságának védelméhez fűződő jogaival szemben, sem pedig a felhasználók általános adatvédelmi rendeletben foglalt adatvédelmi jogaival szemben. A preambulumbekzdésben ezért rögzíteni szükséges minimálisan azt, hogy a szolgáltatónak a tartózkodási helyre vonatkozó adatok, illetve az egyéb metaadatok további kezelése esetén eleget kell tennie az általános adatvédelmi rendelet 25. cikkében foglalt kötelezettségeknek. Ennek keretében legalább a következő intézkedéseket kell alkalmaznia:

- i. ideiglenes álneveket kell használnia;
- ii. törölnie kell az álnevek és az eredeti azonosító adatok visszafelé irányuló összekapcsolását lehetővé tévő táblázatokat;
- iii. az adatokat olyan szinten kell összesítenie, ahol az egyes felhasználók az útvonaluk alapján már nem azonosíthatóak; valamint
- iv. törölnie kell azokat a kiugró adatokat, amelyek esetében továbbra is lehetőség nyílna az azonosításra (mindezen intézkedéseket együttesen kell alkalmazni).

Végül pedig az elektronikus hírközlési adatvédelmi rendeletnek köteleznie kell a tartózkodási helyre vonatkozó, illetve egyéb metaadatok kezelésében részt vevő feleket arra, hogy a jogszabályban garantált titoktartás megsértése nélkül tegyék nyilvánosan megismerhetővé az anonimizáláshoz és további összesítéshez használt módszereiket. Ez lehetővé tenné, hogy mind a

felügyeleti hatóságok, mind a tágabb nyilvánosság könnyen ellenőrizze a választott módszer megfelelőségét.

KÉRETLEN KÖZLÉSEKKEL KAPCSOLATOS PONTOSÍTÁS

43. A munkacsoport az alábbi pontosításokra tesz javaslatot a kérértlen közlések tekintetében:

- a. **A jóváhagyás nélkül végzett közvetlen üzletszerzés tilalmának megfogalmazása.** A javasolt rendelet 16. cikkének (1) bekezdése jelenleg rögzíti, hogy az elektronikus hírközlési szolgáltatások (jóváhagyás megléte esetén) használhatók közvetlen üzletszerzés küldésére, azonban nem tartalmaz a közvetlen üzletszerzés jóváhagyás hiányában történő küldésére (felhasználóra irányítására vagy hozzá intézésére) vonatkozó konkrét tilalmat. Ez ellentétes a más rendelkezésekben alkalmazott megközelítéssel, ahol elsőként a tilalom került megfogalmazásra, és ezt követték a pontosan meghatározott kivételek. A jelenlegi megfogalmazás (valószínűleg nem szándékosan) egy engedékenyebb megközelítést sugall. A munkacsoport a jelenlegi elektronikus hírközlési adatvédelmi irányelv 13. cikkének (1) bekezdése kismértékben módosított szövegének alkalmazását javasolja: „Az elektronikus hírközlési szolgáltatások, köztük a hang alapú hívások, az automatizált hívó- és kommunikációs rendszerek, köztük a hívott személyt más személlyel összekapcsoló, félig automatizált rendszerek, továbbá a faxberendezések, az elektronikus levelek és az egyéb célra használt elektronikus hírközlési szolgáltatások természetes vagy jogi személyek által közvetlen üzletszerzési célból történő használata kizárólag az ahhoz előzetesen hozzájáruló végfelhasználók vonatkozásában lehetséges.”
- b. **A meglévő vevőkhöz intézett üzletszerzési közlésekre és hívásokra vonatkozó rendelkezés hatálya.** A 16. cikk (2) bekezdése rögzíti, hogy a meglévő vevők elektronikus levelezési kapcsolattartási adatainak megszerzése esetén ezek a kapcsolattartási adatok felhasználhatók a saját termékekre és szolgáltatásokra vonatkozó további közvetlen üzletszerzéshez, feltéve, hogy egyértelmű, díjmentes, egyszerűen használható lehetőséget biztosítanak ennek elutasítására mind az adatok megszerzésekor, mind a további üzenetekben. Ez jelenleg a „termék vagy szolgáltatás értékesítésével összefüggésben” megszerzett vevőkre és a saját, hasonló termékek és szolgáltatások további kereskedelmi értékesítésére korlátozódik. Tekintettel arra, hogy a közvetlen üzletszerzésre vonatkozó rendelkezések a nem kereskedelmi népszerűsítési tevékenységekre (pl. jótékony szervezetekre, politikai pártokra) ugyanúgy vonatkoznak, ezt a rendelkezést módosítani kell annak érdekében, hogy a nem kereskedelmi szervezetek által folytatott, korábbi támogatóikra irányuló, saját, hasonló céljaik és elképzeléseiket népszerűsítő megkeresésekre is ugyanúgy vonatkozzon, és ugyanolyan jogot biztosítson ennek elutasítására, mint a közvetlen üzletszerzési hívások tekintetében. Ezen felül korlátozni kell a „meglévő vevői státusz” érvényességi idejét a kereskedelmi, jótékonyági vagy politikai célú elektronikus kommunikáció tekintetében, és ennek a korlátozásnak kell

vonatkoznia a közvetlen üzletszerzési hívásokra is. Amennyiben a tagállam egy hang alapú marketinghívások elutasítására szolgáló rendszert választott, a „meglévő vevői” viszony fennállása felülírja a „Ne hívj” nyilvántartásba történő feliratkozást. Ebben a helyzetben a végfelhasználónak nincs érdemi lehetősége a kéréstlen hívások megakadályozására olyan vállalatoktól és szervezetektől, amelyekkel egykor kapcsolatban álltak, de már nem kívánnak kommunikálni. A rendeletnek ezért alapszabályként meg kell határoznia – például egy vagy két évben – az ilyen „meglévő vevői státuszon” alapuló kivétel érvényességét, figyelemmel az érintett végfelhasználók jogos elvárásaira.

- c. **A közvetlen üzletszerzésre vonatkozó szabályok alkalmazása jogi személyeknél.** A javasolt rendelet 16. cikkének (5) bekezdése rögzíti, hogy a tagállamok gondoskodnak a jogi személyiséggel rendelkező végfelhasználók kéréstlen közlésekkel kapcsolatos jogos érdekeinek megfelelő védelméről. A nem természetes személy előfizetők jogos érdekeit a jelenlegi elektronikus hírközlési adatvédelmi irányelv 13. cikkének (5) bekezdése ismerteti. Nem világos, hogy a megfogalmazás módosítása milyen következményekkel jár. A preambulumbekkezdésekben tisztázni kell, hogy ez a módosítás nem jelent alacsonyabb szintű védelem nyújtására vonatkozó szándékot. Ehhez kapcsolódik, hogy a jóváhagyás hiányában végzett közvetlen üzletszerzés tilalma „a hozzájárulást adó természetes személy végfelhasználókra” vonatkozik (utólagos kiemelés). Egyértelművé kell tenni, hogy ebbe beletartoznak a jogi személyeknek dolgozó természetes személyek. Nem szükséges ellenben jóváhagyás a jogi személyek megkereséséhez akkor, ha az az általuk e célból közzétett általános kapcsolattartási adatok (pl. info@vállalatneve.eu) felhasználásával történik.
- d. **A közvetlen üzletszerzésre vonatkozó szabályok alkalmazása (politikai) képviseleti szerekörben eljáró személyeknél:** Jelenlegi formájában a 16. cikk meggátolhatja bizonyos, kereskedelmi aggályokat vagy érdekeket ismertető közlések választott képviselőknek történő elküldését. Tisztázni kell, hogy a rendelet nem gátolja meg az ilyen közléseket.

AZ ALAPVETŐ JOGOKAT RÖGZÍTŐ JOGI AKTUSOK ALKALMAZÁSÁNAK PONTOSÍTÁSA

- 44. Pontosításra szorul a **Charta és az EJEE nemzeti adatmegőrzési jogszabályok tekintetében való alkalmazása**. A (26) preambulumbekkezdés rögzíti, hogy a tagállamok közérdek védelmét szolgáló, például a jogszerű lehallgatást lehetővé tévő intézkedéseinek (az EJEE mellett) összhangban kell lenniük a Chartával. Ez kívánatos, mert a *Tele2/Watson* indoklásával összhangban áll, hogy az uniós jog által biztosított, adatkezeléssel kapcsolatos védelem alóli nemzeti kivételek a Charta hatálya alá esnek (és a nemzeti jogszabályok által megvalósított jogsértés ennek megfelelően az EU Bírósága elé vihető). A javasolt rendelet 11. cikke azonban csupán azt említi, hogy a javasolt rendelet 5-8. cikkei hatályának esetleges korlátozásakor tiszteletben kell tartani az alapvető jogok és szabadságok lényegét, és hogy az intézkedésnek szükségesnek és arányosnak kell lennie. Itt a Chartára és az EJEE-re vonatkozó kifejezett hivatkozásnak is szerepelnie kell.

45. **A közlés bizalmasságát az EEJE 8. cikke is védi.** Az indoklás 1.1 pontja és az (1) preambulumbekkezdés rögzíti, hogy a javasolt rendelet a Charta 7. cikkét hajtja végre. Ezt a (19) preambulumbekkezdés is megismétli. A közlés bizalmasságához fűződő alapvető jogot azonban nem csak ez a rendelkezés, hanem az EEJE 8. cikke is védi. Az erre vonatkozó konkrét hivatkozás szerepeltetése a javasolt rendelet valamely cikkében még inkább megerősítené, hogy a (végleges) rendelet értékelésénél figyelembe kell venni az Emberi Jogok Európai Bíróságának releváns joggyakorlatát. Ez a hivatkozás egyébként már szerepel a (végberendezésekre vonatkozó) (20) preambulumbekkezdésben és a (jogszerű lehallgatásra vonatkozó) (26) preambulumbekkezdésben, valamint támogatják az indoklás 2.1 pontjában foglalt (jogi személyek esetében a Charta és az EEJE között fennálló viszonyra vonatkozó) szempontok, azonban a releváns cikkek, például a 11. cikk (1) bekezdése nem tartalmazza.

EGYÉB PONTOSÍTÁSOK

46. Tisztázni kell, hogy a személyes adatokat tartalmazó elektronikus kommunikációs adatok kezelése esetén **az általános adatvédelmi rendeletben előírt, például az adatvédelmi incidensekre és az adatvédelmi hatásvizsgálatra vonatkozó kötelezettségek továbbra is érvényben maradnak.** Miután az (5) preambulumbekkezdés említi, hogy a javasolt rendelet az általános adatvédelmi rendelethez kapcsolódó *lex specialis*, és hogy az elektronikus kommunikációs adatok kezelése csak a javasolt rendeletben foglaltakkal összhangban engedhető meg, kétség merülhet fel arra vonatkozóan, hogy az általános adatvédelmi rendeletben előírt bizonyos kötelezettségek a javasolt rendelet tekintetében is alkalmazandók-e. Különösen igaz ez azokra az esetekre, ahol a javasolt rendelet egy bizonyos kötelezettség előírásaként értelmezhető, miközben az általános adatvédelmi rendelet szintén szabályozza a adott kérdést. Például:

- (i) a javasolt rendelet bizonyos értesítést ír elő az „észlelt” biztonsági kockázatokról (17. cikk) (lásd a 35. megjegyzést is), azonban az általános adatvédelmi rendelet tartalmazza az adatvédelmi incidensekről nyújtandó értesítések szabályozását (33. és 34. cikk);
- (ii) A javasolt rendelet megemlíti, hogy bizonyos körülmények esetén kötelező az általános adatvédelmi rendeletnek megfelelő adatvédelmi hatásvizsgálat elvégzése, illetve a felügyeleti hatósággal való konzultáció ((17) és (19) preambulumbekkezdés, valamint 6. cikk (3) bek. b) pont), miközben az általános adatvédelmi rendelet már rögzíti, hogy mikor kell adatvédelmi hatásvizsgálatot, illetve konzultációt folytatni (35. és 36. cikk), és;
- (iii) Nincs kimondva, hogy az adatkezelés tilalma alóli, a javasolt rendelet 5. cikkében foglalt valamely kivétel feltételeinek való megfelelés esetén is elegendő tenni az általános adatvédelmi rendeletben előírt valamennyi vonatkozó kötelezettségnek a személyes adatok kezelése tekintetében, és hogy az általános adatvédelmi rendelet szerinti minden egyéb adatkezelés tilos. Tisztázni kell, hogy az általános adatvédelmi rendelet 6. cikkének (4) bekezdésében szereplő összeegyeztethetőségi vizsgálat nem alkalmazható.

- (iv) A javasolt elektronikus hírközlési adatvédelmi rendelet nem tesz lehetővé az általános adatvédelmi rendelet 42. és 43. cikkében foglalt tanúsítási mechanizmusokat. Mivel az általános adatvédelmi rendelet 42. cikkének hatálya szigorúan tekintve az olyan adatvédelmi tanúsítási mechanizmusok, valamint adatvédelmi bélyegzők, illetve jelölések létrehozására korlátozódik, amelyek célja az általános adatvédelmi rendeletnek való megfelelés bizonyítása, megfontolandó, hogy nincs-e szükség egy hasonló rendelkezés bevezetésére, amely lehetővé tenné annak tanúsítását, hogy az adott adatkezelési művelet, szabvány, termék vagy szolgáltatás megfelel az elektronikus hírközlési adatvédelmi rendeletben foglaltaknak.

Annak érdekében, hogy az erre vonatkozó egyértelműség hiánya ne legyen felhasználható a javasolt rendelet által biztosított védelem szintjének csökkentéséhez, egyértelművé kell tenni, hogy az adatkezelőknek minden ilyen esetben meg kell felelniük az általános adatvédelmi rendeletben foglaltaknak is.

47. Tisztázni szükséges továbbá, **hogy a hozzájárulás visszavonására vonatkozó követelmény a végberendezéseket érintő beavatkozás esetén is fennáll.** A javasolt rendelet 8. cikke (1) bekezdésének b) pontja lehetőséget biztosít a végfelhasználó végberendezésének működésébe való beavatkozásra, ha ahhoz a végfelhasználó hozzájárul. A 9. cikk (3) bekezdése rögzíti, hogy a végfelhasználók számára lehetőséget kell biztosítani arra, hogy hozzájárulásukat bármikor visszavonják, ez azonban csak a metaadatok és a tartalmak elemzéséhez való hozzájárulásra vonatkozik. Tisztázni kell, hogy ez a kötelezettség a végberendezéseket érintő beavatkozásra is kiterjed.
48. Ehhez kapcsolódóan tisztázni kell azt is, **hogy a hozzájárulás visszavonásának lehetőségére vonatkozó emlékeztető a böngésző beállításai révén megadott hozzájárulásra is vonatkozik.** A 9. cikk (3) bekezdése értelmében a végfelhasználókat rendszeres időközönként, 6 havonta emlékeztetni kell arra, hogy hozzájárulásukat bármikor visszavonhatják. Bár a munkacsoport úgy ítéli meg, hogy a böngészők és más szoftverek, köztük az operációs rendszerek, az alkalmazások, valamint a tárgyak internetéhez csatlakozó eszközök kapcsolódási felületét biztosító szoftverek általános (azaz specifikus, részletes szabályozást lehetővé nem tévő) beállításai nem képezhetik a hozzájárulás megadásának érvényes módját, mivel az általános beállítások nem alkalmasak különféle helyzetekre vonatkozóan eltérő hozzájárulás megadására (lásd a 24. megjegyzést), az alapértelmezett beállításoknak felhasználóbarátnak kell lenniük (lásd a 19. megjegyzést). *Amennyiben* ez benne marad a javasolt rendeletben, a beállításoknak kellően nagy felbontásúnak kell lenniük ahhoz, hogy szabályozzák mindazon adatkezelést, amelyhez a felhasználó a hozzájárulását adja, és hogy kiterjedjenek a berendezés minden olyan funkciójára, amely adatkezeléshez vezethet. Emellett a végfelhasználókat legalább időszakosan (6 havonta) emlékeztetni kell arra, hogy ezeket a beállításokat megváltoztathatják.
49. Üdvözlendő, hogy a javasolt rendelet előírja a már forgalomba hozott szoftverek számára, hogy tájékoztassák a végfelhasználót az adatvédelmi beállítási lehetőségeikről (10. cikk). **Nem világos azonban, hogy ez hogyan érvényesíthető érdemben a korábbi, illetve a már nem támogatott termékeknél.** Pontosítani kellene

továbbá, hogy ez a kötelezettség hogyan alkalmazandó a nyitott, decentralizált fejlesztésű, nyílt forráskódú szoftverek esetében.

50. Tisztázni kell, hogy a **(harmadik felektől származó) sütik tiltására vonatkozó, a javasolt rendelet 10. cikke szerinti lehetőség felkínálása elsőbbséget élvez a 8. cikk (1) bekezdésének d) pontja szerinti online közönségméréssel szemben.** Más szóval: ha a honlap a 8. cikk (1) bekezdésének d) pontja alapján analitikai eszközöket használ az online közönség mérése céljából, a felhasználónak akkor is joga van ezeket a nyomonkövetési technológiákat a böngészőjében letiltani.
51. Pontosításra szorul a **(félig) automatizált hívó- és kommunikációs rendszerek meghatározása.** A javasolt rendelet 4. cikke (3) bekezdésének h) pontjában megadott, e fogalomra vonatkozó meghatározás a mondat második felében magára a meghatározott fogalomra hivatkozik („ideértve a hívott felet személyhez kapcsoló automatizált hívó- és hírközlő rendszerekkel bonyolított hívásokat is”). Javasoljuk ennek az utolsó mondatnak a törlését a meghatározásból, és a 4. cikk (3) bekezdésének g) pontjában szereplő fogalom meghatározás módosítását úgy, hogy az magában foglalja a hívott felet személyhez kapcsoló automatizált hívó- és hírközlő rendszerek, például automata tárcsázók segítségével végrehajtott hívásokat.
52. Pontosításra szorul, **mi értendő a „szolgáltatásra való előfizetés részét képező” információ alatt.** A (14) preambulumbekkezdés megemlíti, hogy az elektronikus kommunikációs metaadatok között „az adott szolgáltatásra való előfizetés részét képező információk is szerepelhetnek, ha ezeket az információkat az elektronikus hírközlés tartalmának továbbítása, terjesztése vagy cseréje céljából kezelik”. E szövegrész célja nem világos.
53. Tisztázni kell **az egységességi és az együttműködési mechanizmusok alkalmazását.** A (38) preambulumbekkezdés rögzíti, hogy a javasolt rendelet az általános adatvédelmi rendeletben előírt egységességi mechanizmusra támaszkodik. A 18. cikk (1) bekezdése ehhez hozzáteszi, hogy az általános adatvédelmi rendelet VI. és VII. fejezetét értelemszerűen kell alkalmazni. A 19. cikk rögzíti továbbá, hogy az Európai Adatvédelmi Testület (EDPB) ellátja az általános adatvédelmi rendelet 70. cikkében rögzített feladatokat. Bár e rendelkezések alkalmazása viszonylag egyértelmű, nem zárható ki, hogy az értelmezéssel kapcsolatos kérdés merül fel az általános adatvédelmi rendeletben előírt egységességi és együttműködési mechanizmusok tekintetében. A „határokon átnyúló adatkezelés” tekintetében például a fő felügyeleti hatóságra vonatkozó mechanizmust kell alkalmazni (általános adatvédelmi rendelet 56. cikk (1) bek.), de nem egyértelmű, hogyan vonatkozik ez a végberendezéseket érintő beavatkozások vagy a tartalom, illetve metaadatok elemzése esetére a javasolt rendelet szerint. Ezért tanácsos lenne ezeknek a kulcsfogalmaknak az alkalmazását egy preambulumbekkezdésben tisztázni, kiemelve, hogy az általános adatvédelmi rendelet érintett fejezetei javasolt rendelettel összefüggésben történő alkalmazásával kapcsolatban fennmaradó kérdéseket az adott fejezetnek a rendeltetésével összhangban történő értelmezése útján kell feloldani. Tanácsos lenne azt is pontosítani, hogy a javasolt rendelettel összefüggésben a 70. cikket értelemszerűen kell alkalmazni az Európai Adatvédelmi Testületre (ez jelenleg hiányzik a preambulumbekkezdésből).

* * *