Iránymutatások

# 2/2023. sz. iránymutatás az elektronikus hírközlési adatvédelmi irányelv 5. cikke (3) bekezdésének műszaki hatályáról

## 2.0 változat

## Elfogadás időpontja: 2024. október 7.

Translations proofread by EDPB Members.

This language version has not yet been proofread.

*Korábbi változatok*

| | | |
|---|---|---|
| 1.0 változat | 2023. november 14. | Az iránymutatás nyilvános konzultáció céljából történő elfogadása |
| 2.0 változat | 2024. október 7. | Az iránymutatás nyilvános konzultációt követő elfogadása |

**Összefoglaló**

Ebben az iránymutatásban az Európai Adatvédelmi Testület az elektronikus hírközlési adatvédelmi irányelv 5. cikke (3) bekezdésének különböző műszaki megoldásokra való alkalmazhatóságával foglalkozik. Ez az iránymutatás a 29. cikk szerinti munkacsoportnak az elektronikus hírközlési adatvédelmi irányelvnek az eszköz-ujjlenyomatvételre való alkalmazásáról szóló 9/2014. számú véleményét egészíti ki, és célja, hogy világos képet adjon az elektronikus hírközlési adatvédelmi irányelv 5. cikke (3) bekezdésének hatálya alá tartozó műszaki műveletekről.

Kritikus adatvédelmi aggállyá vált olyan új nyomonkövetési módszerek megjelenése, amelyek egyrészt felváltják a meglévő nyomkövető eszközöket (például a sütiket, mivel néhány böngészőértékesítő már nem támogatja a harmadik felektől származó sütiket), másrészt új üzleti modelleket hoznak létre. Míg az elektronikus hírközlési adatvédelmi irányelv 5. cikke (3) bekezdésének alkalmazása elfogadott és megvalósul egyes nyomonkövetési technológiák, például a sütik esetében, kezelni kell az említett rendelkezés új nyomkövető eszközökre történő alkalmazásával kapcsolatos bizonytalanságokat.

Az iránymutatás az elektronikus hírközlési adatvédelmi irányelv 5. cikke (3) bekezdése alkalmazhatóságának alábbi három kulcsfontosságú elemét azonosítja (2.1. szakasz): „adatok”, „egy előfizető vagy felhasználó végberendezése”, valamint „adattárolás és a tárolt adatokhoz való hozzáférés”. Az iránymutatás részletesen elemzi továbbá az egyes elemeket (2.2–2.6. szakasz).

A 3. szakasz ezt az elemzést az általános technikákat jelképező felhasználási esetek alábbi példáira alkalmazza:

- URL-es és pixeles nyomon követés
- helyi feldolgozás
- kizárólag IP-n alapuló nyomon követés
- a dolgok internetével (IoT) kapcsolatos időszakos és közvetített jelentés
- egyedi azonosító

# Tartalomjegyzék

## Az Európai Adatvédelmi Testület,

tekintettel 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 szóló, 2016. április 27-i (EU) 2016/679 európai parlamenti és tanácsi rendelet (a továbbiakban: általános adatvédelmi rendelet) 70. cikke (1) bekezdésének e) pontjára,

tekintettel az EGT-megállapodásra és különösen annak az EGT Vegyes Bizottság 2018. július 6-i 154/2018 határozatával módosított XI. mellékletére és 37. jegyzőkönyvére[1],

tekintettel a 2009/136/EK irányelvvel módosított, az elektronikus hírközlési ágazatban a személyes adatok kezeléséről, feldolgozásáról és a magánélet védelméről szóló, 2002. július 12-i 2002/58/EK európai parlamenti és tanácsi irányelv (a továbbiakban: elektronikus hírközlési adatvédelmi irányelv) 15. cikkének (3) bekezdésére,

tekintettel eljárási szabályzatának 12. és 22. cikkére,

**ELFOGADTA A KÖVETKEZŐ IRÁNYMUTATÁST:**

# 1 BEVEZETÉS

1. Az elektronikus hírközlési adatvédelmi irányelv 5. cikkének (3) bekezdése szerint *„egy előfizető vagy felhasználó végberendezésében történő adattárolás, illetve az ott tárolt adatokhoz való hozzáférés”* csak előzetes hozzájárulás vagy az e cikkben meghatározott konkrét célokra való szükségesség alapján megengedett. Amint arra az elektronikus hírközlési adatvédelmi irányelv (24) preambulumbekezdése[2] emlékeztet, az említett rendelkezés célja a felhasználók végberendezéseinek védelme, mivel azok a felhasználók magánszférájának részét képezik. A cikk szövegéből következik, hogy az elektronikus hírközlési adatvédelmi irányelv 5. cikkének (3) bekezdése nem kizárólag a sütikre vonatkozik, hanem a „hasonló technológiákra” is. Jelenleg azonban nem áll rendelkezésre átfogó lista az elektronikus hírközlési adatvédelmi irányelv 5. cikke (3) bekezdésének hatálya alá tartozó műszaki műveletekről.

2. A 29. cikk szerinti munkacsoportnak az elektronikus hírközlési adatvédelmi irányelvnek az eszköz-ujjlenyomatvételre való alkalmazásáról szóló 9/2014. számú véleménye (a továbbiakban: a 29. cikk szerinti munkacsoport 9/2014. sz. véleménye) már egyértelművé tette, hogy az ujjlenyomatvétel az elektronikus hírközlési adatvédelmi irányelv 5. cikke (3) bekezdésének műszaki hatálya alá tartozik[3], de az új technológiai fejlesztések miatt további iránymutatásra van szükség a jelenleg megfigyelhető nyomonkövetési technikákat illetően. A műszaki környezet fejlődött az elmúlt évtizedben az operációs

[1] Az ebben a dokumentumban a „tagállamokra” történő bármely hivatkozást „EGT-tagállamokra” történő hivatkozásként kell érteni.

[2] „Az elektronikus hírközlő hálózatok felhasználóinak végberendezései és az azokon tárolt minden adat a felhasználók magánszférájának részét képezi, amelynek az Emberi jogok és alapvető szabadságok védelméről szóló európai egyezmény alapján védelmet kell élveznie. Az úgynevezett kémszoftverek, web-poloskák, rejtett azonosítók és egyéb hasonló eszközök a felhasználó tudta nélkül bejuthatnak a felhasználó végberendezésébe adatszerzés, rejtett adatok tárolása vagy a felhasználó tevékenységeinek nyomon követése céljából, és súlyosan sérthetik e felhasználóknak a magánélet tiszteletben tartásához való jogát. Az ilyen eszközök alkalmazását kizárólag törvényes célból, az érintett felhasználók tudtával lehet engedélyezni.”

[3] A 29. cikk szerinti munkacsoport 9/2014. sz. véleménye, 11. o.

rendszerekbe beágyazott azonosítók növekvő mértékű használata, valamint a végberendezésekben történő adattárolást lehetővé tevő új eszközök létrehozása révén.

3. Az elektronikus hírközlési adatvédelmi irányelv 5. cikke (3) bekezdésének hatályával kapcsolatos bizonytalanságok ösztönözték az internetfelhasználók nyomon követésére szolgáló alternatív megoldások alkalmazását, és az elektronikus hírközlési adatvédelmi irányelv 5. cikkének (3) bekezdésében előírt jogi kötelezettségek megkerülésére irányuló tendenciához vezettek. Minden ilyen helyzet aggályokat vet fel, és további elemzést igényel az Európai Adatvédelmi Testület korábbi iránymutatásának kiegészítése érdekében.

4. Ezen iránymutatás célja az elektronikus hírközlési adatvédelmi irányelv 5. cikke (3) bekezdésének hatályára vonatkozó műszaki elemzés elvégzése, nevezetesen annak tisztázása, hogy műszaki szempontból mit takar az *„egy előfizető vagy felhasználó végberendezésében történő adattárolás, illetve az ott tárolt adatokhoz való hozzáférés”* kifejezés. Ez az iránymutatás nem foglalkozik azokkal a körülményekkel, amelyek fennállása esetén egy adatkezelési művelet az előzetes hozzájárulás követelménye alól az elektronikus hírközlési adatvédelmi irányelv által előírt kivételek[4] hatálya alá tartozhat, mivel e körülményeket eseti alapon kell elemezni, figyelembe véve a vonatkozó tagállami átültető intézkedés(eke)t és az illetékes nemzeti hatóságok által kiadott iránymutatást.

5. A konkrét felhasználási esetek nem kimerítő felsorolása ezen iránymutatás utolsó részében kerül elemzésre.

# 2 ELEMZÉS

## 2.1 Az elektronikus hírközlési adatvédelmi irányelv 5. cikke (3) bekezdése alkalmazhatóságának kulcsfontosságú elemei

6. Az elektronikus hírközlési adatvédelmi irányelv 5. cikkének (3) bekezdése akkor alkalmazandó, ha:

   a. **A. KRITÉRIUM:** a végzett műveletek *„adatokkal”* kapcsolatosak. Meg kell jegyezni, hogy a használt kifejezés nem „személyes adatok”, hanem „adatok”.

   b. **B. KRITÉRIUM:** a végzett műveletek egy előfizető vagy felhasználó *„végberendezését"* érintik (B.1.), ami szükségessé teszi a *„nyilvános hírközlő hálózat”* fogalmának értékelését (B.2.).

   c. **C. KRITÉRIUM:** a végzett műveletek ténylegesen *„tárolásnak”* (C.1.) vagy *„hozzáférésnek”* (C.2.) minősülnek. E két fogalom önállóan vizsgálható, amint arra a 29. cikk szerinti munkacsoport 9/2014. sz. véleménye is emlékeztet: *„A »tárol vagy hozzáfér« szavak azt jelentik, hogy a tárolásnak és a hozzáférésnek nem kell ugyanazon közlés során megtörténnie, és azokat nem kell ugyanannak a félnek végrehajtania.”*[5]

Az érthetőség kedvéért a felhasználó végberendezésében tárolt adatokhoz hozzáférő szervezetre ez az iránymutatás a továbbiakban „hozzáférő szervezet”-ként hivatkozik.

[4] Az elektronikus hírközlési adatvédelmi irányelv 5. cikkének (3) bekezdése értelmében: *„Ez a rendelkezés nem akadályozza az olyan műszaki tárolást, illetve műszaki hozzáférést, amelynek kizárólagos célja az elektronikus hírközlő hálózaton keresztül történő közléstovábbítás, vagy amelyre az előfizető vagy felhasználó által kifejezetten kért, az információs társadalommal összefüggő szolgáltatás nyújtásához a szolgáltatónak feltétlenül szüksége van.”*

[5] A 29. cikk szerinti munkacsoport 9/2014. sz. véleménye, 8. o.

## 2.2 Az „adatok” fogalma – A. kritérium

7. Az A. kritérium kapcsán kifejtetteknek megfelelően e szakasz azt részletezi, hogy mit foglal magában az „adatok” fogalma. A „személyes adatok” fogalmánál tágabb kategóriát magában foglaló „adatok” kifejezés használata melletti döntés az elektronikus hírközlési adatvédelmi irányelv hatályához kapcsolódik.

8. Az elektronikus hírközlési adatvédelmi irányelv 5. cikke (3) bekezdésének célja a felhasználók magánszférájának védelme, amint azt a (24) preambulumbekezdés is kimondja: *„Az elektronikus hírközlő hálózatok felhasználóinak végberendezései és az azokon tárolt minden adat a felhasználók magánszférájának részét képezi, amelynek az Emberi jogok és alapvető szabadságok védelméről szóló európai egyezmény alapján védelmet kell élveznie.”* A magánszférát az Európai Unió Alapjogi Chartájának 7. cikke is védelemben részesíti.

9. Ami azt illeti, az elektronikus hírközlési adatvédelmi irányelv 5. cikke (3) bekezdésének és (24) preambulumbekezdésének szövege kifejezetten vonatkozik azokra a helyzetekre, amelyekben – akár személyes adatok érintettsége nélkül is – beavatkozás történik ebbe a magánszférába, így például vírusoknak a felhasználó végberendezésén történő tárolására. Ez azt mutatja, hogy az „adatok” fogalmának meghatározása nem korlátozódhat arra a tulajdonságra, hogy az adatok azonosított vagy azonosítható természetes személyre vonatkoznak.

10. Ezt az Európai Unió Bírósága is megerősítette: *„Ez a védelem minden olyan adatra vonatkozik, amelyet e végberendezésen tárolnak, függetlenül attól, hogy személyes adatokról van-e szó, vagy sem, és – amint ugyanezen preambulumbekezdésből kitűnik – különösen arra irányul, hogy megvédje a felhasználókat annak veszélyével szemben, hogy rejtett azonosítók vagy egyéb hasonló eszközök e felhasználók tudtán kívül bejussanak a végberendezéseikbe.”*[6]

11. Korábban már tisztázásra került a kérdés, hogy ezen adatok eredetét és a végberendezésben történő tárolásának okát figyelembe kell-e venni az elektronikus hírközlési adatvédelmi irányelv 5. cikke (3) bekezdése alkalmazhatóságának értékelése során. A 29. cikk szerinti munkacsoport 9/2014. sz. véleménye szerint például: *„Nem helyes ezt úgy értelmezni, mintha azt jelentené, hogy a harmadik félnek nem kell hozzájárulást beszereznie az ilyen információhoz való hozzáféréshez egyszerűen azért, mert nem ő tárolta azt. A hozzájárulás beszerzésének kötelezettsége irányadó akkor is, ha csak olvasható értékhez férnek hozzá (pl. egy hálózati interfész MAC címének lekérése az operációs rendszer API-ján keresztül).”*[7]

12. Az „adatok” fogalma következésképpen magában foglalja mind a nem személyes adatokat, mind a személyes adatokat függetlenül attól, hogy hogyan és ki – azaz egy külső szervezet (beleértve a hozzáféréssel rendelkező szervezettől eltérő szervezeteket is), a felhasználó, egy gyártó vagy bárki más – tárolta ezeket az adatokat.

## 2.3 Az „egy előfizető vagy felhasználó végberendezése” fogalma – B.1. kritérium

13. Ez a szakasz a 2008/63/EK irányelvben használt és az (EU) 2018/1972 irányelv 2. cikkében hivatkozott fogalommeghatározásra épül, amely szerint a „végberendezés” *„olyan, információk küldésére, feldolgozására vagy vételére szolgáló berendezés, amely valamely nyilvános távközlési hálózat interfészéhez közvetlenül vagy közvetve kapcsolódik; mind közvetlen, mind közvetett csatlakozások esetében az összeköttetés vezetékes, száloptikás vagy elektromágneses módszerrel építhető ki;*

[6] A Bíróság 2019. október 1-jei ítélete, Planet 49, C-673/17, ECLI:EU:C:2019:801, 70. pont.
[7] A 29. cikk szerinti munkacsoport 9/2014. sz. véleménye, 8. o.

*közvetett csatlakozás esetében a végberendezés és a nyilvános hálózati interfész között még egy berendezés helyezkedik el”*[8].

14. Az elektronikus hírközlési adatvédelmi irányelv (24) preambulumbekezdése egyértelművé teszi a végberendezésnek az elektronikus hírközlési adatvédelmi irányelv 5. cikkének (3) bekezdése által nyújtott védelem szempontjából betöltött szerepét. Az elektronikus hírközlési adatvédelmi irányelv nemcsak adataik titkossága tekintetében védi a felhasználók magánéletét, hanem a felhasználó végberendezése integritásának védelme révén is. Ez a felfogás vezérli a „végberendezés” fogalmának értelmezését ezen iránymutatásban.

15. Az elektronikus hírközlési adatvédelmi irányelv 3. cikke szerint ezen irányelv alkalmazhatóságához a személyes adatok kezelésének nyilvánosan elérhető hírközlési szolgáltatások nyilvános hírközlő hálózaton történő nyújtásával kell összefüggnie. Ez azt jelenti, hogy egy eszköznek ilyen szolgáltatással összefüggésben kell használhatónak lennie, és hogy ahhoz, hogy végberendezésnek minősüljön, kapcsolódnia kell egy nyilvános hírközlő hálózat interfészéhez, vagy összekapcsolhatónak[9] kell lennie azzal. Az Európai Adatvédelmi Testület megjegyzi, hogy az elektronikus hírközlési adatvédelmi irányelv 5. cikke (3) bekezdésének szövegében 2009-ben végrehajtott módosítások[10] kiterjesztették a végberendezések védelmét azáltal, hogy törölték az „elektronikus hírközlő hálózatoknak” a végberendezésben történő adattárolásra, illetve az ott tárolt adatokhoz való hozzáférésre való „felhasználására” való hivatkozást. Ezért amennyiben az eszköz olyan hálózati interfésszel rendelkezik, amely alkalmassá teszi a kapcsolódásra (még ha nem valósul is meg ilyen kapcsolódás), az elektronikus hírközlési adatvédelmi irányelv 5. cikkének (3) bekezdése minden olyan szervezetre alkalmazandó, amely a végberendezésben adatokat tárolna, vagy hozzáférne az ott tárolt adatokhoz, függetlenül a végberendezéshez való hozzáférés módjától és attól, hogy a végberendezés kapcsolódik-e vagy sem egy hálózathoz.

16. Azok a berendezések, amelyek magának a nyilvános elektronikus hírközlő hálózatnak a részét képezik, nem minősülnek az elektronikus hírközlési adatvédelmi irányelv 5. cikkének (3) bekezdése értelmében vett végberendezésnek[11].

17. A végberendezés bármilyen számú egyedi hardverből állhat, amelyek együttesen alkotják a végberendezést. Ez lehet egy fizikailag zárt eszköz, amely az összes megjelenítő, feldolgozó, tároló és perifériás hardvert magában foglalja (például okostelefonok, laptopok, hálózathoz csatlakoztatott tárolóeszközök, hálózatba kapcsolt autók vagy hálózatba kapcsolt televíziók, intelligens szemüvegek).

18. Az elektronikus hírközlési adatvédelmi irányelv elismeri, hogy a felhasználó végberendezésében tárolt adatok titkosságának és a felhasználó végberendezése integritásának védelme nem korlátozódik a

[8] A Bizottság 2008/63/EK irányelve (2008. június 20.) a távközlési végberendezések piacán folyó versenyről (kodifikált változat), az 1. cikk 1. pontja.

[9] Vagyis rendelkeznie kell a hálózathoz való kapcsolódáshoz szükséges műszaki képességekkel, még ha a kapcsolódás éppen nem valósul is meg.

[10] Az Európai Parlament és a Tanács 2009/136/EK irányelve (2009. november 25.) az egyetemes szolgáltatásról, valamint az elektronikus hírközlő hálózatokhoz és elektronikus hírközlési szolgáltatásokhoz kapcsolódó felhasználói jogokról szóló 2002/22/EK irányelv, az elektronikus hírközlési ágazatban a személyes adatok kezeléséről, feldolgozásáról és a magánélet védelméről szóló 2002/58/EK irányelv és a fogyasztóvédelmi jogszabályok alkalmazásáért felelős nemzeti hatóságok közötti együttműködésről szóló 2006/2004/EK rendelet módosításáról (EGT-vonatkozású szöveg), HL L 337., 2009.12.18., a 2. cikk 5. pontja és a (65) preambulumbekezdés.

[11] A hálózat korlátainak különböző összefüggésekben történő azonosításához lásd a BEREC-nek a hálózati végpontok különböző hálózati topológiák esetében történő meghatározásával kapcsolatos közös megközelítésmódokról szóló iránymutatásait (BoR (20) 46).

természetes személyek magánszférájának védelmére, hanem a a levéltitokhoz való jogukat, illetve a jogi személyek[12] jogos érdekeit is érinti. Így az elektronikus hírközlési adatvédelmi irányelv 5. cikkének (3) bekezdése védi az olyan végberendezést, amely lehetővé teszi ezt a levelezést és a jogi személyek jogos érdekeinek érvényesítését.

19. A felhasználó vagy előfizető tulajdonolhatja vagy bérelheti a végberendezést, vagy más módon kerülhet a birtokába annak. Több felhasználó vagy előfizető meg is oszthatja egymással ugyanazt a végberendezést.

20. E védelmet a felhasználóhoz vagy előfizetőhöz köthető végberendezés számára biztosítja az elektronikus hírközlési adatvédelmi irányelv, és az nem függ attól, hogy a felhasználó tette-e lehetővé a hozzáférést (például az elektronikus hírközlés kezdeményezésével), illetve még attól sem, hogy a felhasználó tudatában van-e az említett hozzáférési lehetőségnek.

## 2.4 A „nyilvános hírközlő hálózat" fogalma – B.2. kritérium

21. Mivel az elektronikus hírközlési adatvédelmi irányelv által szabályozott helyzet *„a Közösségben a nyilvánosan elérhető hírközlési szolgáltatások nyilvános hírközlő hálózaton […] történő nyújtásá[hoz]"*[13] kapcsolódik, és a „végberendezés" fogalmának meghatározása kifejezetten említi a *„nyilvános hírközlő hálózat*" fogalmát, e fogalom tisztázása alapvető jelentőséggel bír azon kontextus meghatározása szempontjából, amelyben az elektronikus hírközlési irányelv 5. cikkének (3) bekezdését alkalmazni kell.

22. Az „elektronikus hírközlő hálózat" fogalmát nem határozza meg maga az elektronikus hírközlési adatvédelmi irányelv. E fogalmat eredetileg az elektronikus hírközlő hálózatok és elektronikus hírközlési szolgáltatások közös keretszabályozásáról szóló 2002/21/EK irányelv („Keretirányelv")[14] határozta meg, amely fogalommeghatározást később felváltotta a 2018/1972 irányelv (Európai Elektronikus Hírközlési Kódex) 2. cikkének 1. pontja. Az jelenleg a következőképpen szól:

> *„elektronikus hírközlő hálózat": olyan átviteli rendszerek összessége – függetlenül attól, hogy állandó infrastruktúrán vagy központi adminisztratív kapacitáselosztáson alapul – és adott esetben kapcsoló vagy útválasztó eszközök, valamint egyéb erőforrások – ideértve a nem aktív hálózati elemeket is –, amelyek jelek továbbítását teszik lehetővé a vezetéken, rádióhullámon, optikai vagy egyéb elektromágneses úton, beleértve a műholdas hálózatokat, az állandóhelyű (vonal- és csomagkapcsolt, beleértve az Internetet) és mozgó hálózatokat, az elektromos vezetékrendszereket, annyiban, amennyiben azokat jelek továbbítására használják, a rádióműsor- és televízióműsor-terjesztő hálózatokat, valamint a kábeltelevízió-hálózatokat, a továbbított információtípusra való tekintet nélkül*[15].

23. E fogalommeghatározás semleges az átviteli technológiák szempontjából. E fogalommeghatározás szerint elektronikus hírközlő hálózat bármely olyan hálózati rendszer, amely lehetővé teszi elektronikus jelek továbbítását a csomópontjai között, függetlenül a használt berendezéstől és protokolloktól.

---

[12] Amint arra ugyanis az Európai Elektronikus Hírközlési Kódex létrehozásáról szóló, 2018. december 11-i (EU) 2018/1972 európai parlamenti és tanácsi irányelv 2. cikkének 13. pontja emlékeztet, a felhasználó természetes személy vagy jogi személy lehet.

[13] Az elektronikus hírközlési adatvédelmi irányelv 3. cikke.

[14] Az Európai Parlament és a Tanács 2002/21/EK irányelve (2002. március 7.) az elektronikus hírközlő hálózatok és elektronikus hírközlési szolgáltatások közös keretszabályozásáról („Keretirányelv").

[15] Az Európai Parlament és a Tanács (EU) 2018/1972 irányelve (2018. december 11.) az Európai Elektronikus Hírközlési Kódex létrehozásáról (átdolgozás) (EGT-vonatkozású szöveg), a 2. cikk 1. pontja.

24. Az elektronikus hírközlő hálózatnak a 2018/1972 irányelv szerinti fogalma nem függ az infrastruktúra állami vagy magánjellegétől, illetve a hálózat kiépítésének vagy kezelésének módjától (*„függetlenül attól, hogy állandó infrastruktúrán vagy központi adminisztratív kapacitáselosztáson alapul”*[16]). Az „elektronikus hírközlő hálózat” fogalmának a 2018/1972 irányelv 2. cikkében szereplő meghatározása ennélfogva kellően tág ahhoz, hogy bármilyen típusú infrastruktúrát magában foglaljon. Az magában foglalja az üzemeltető vagy a nem az üzemeltető által kezelt hálózatokat, az üzemeltetők egy csoportja által közösen kezelt hálózatokat vagy akár az olyan ad hoc hálózatokat is, amelyekben egy végberendezés rövid hatótávolságú átviteli protokollok használatával dinamikusan csatlakozhat más végberendezések hálójához, vagy lecsatlakozhat arról.

25. A „hálózat” fogalmának e meghatározása semmilyen korlátozást nem tartalmaz a hálózatban mindenkor jelen lévő végberendezések számát illetően. Egyes hálózati rendszerek olyan csomópontokra támaszkodnak, amelyek ad hoc módon továbbítanak adatokat az éppen csatlakoztatott csomópontokhoz[17], és azok keretében egy adott időpontban akár csupán csak két tag is kommunikálhat egymással. Az ilyen esetek az elektronikus hírközlési adatvédelmi irányelv általános hatálya alá tartoznak, amennyiben a hálózati protokoll lehetővé teszi további tagok bevonását.

26. A hírközlő hálózat nyilvános elérhetősége szükséges ahhoz, hogy az eszközt végberendezésnek lehessen tekinteni, és következésképpen az elektronikus hírközlési adatvédelmi irányelv 5. cikke (3) bekezdésének alkalmazhatóságához. Meg kell jegyezni, hogy az a körülmény, hogy a hálózat a nyilvánosság korlátozott része (például jogosultsági feltételekhez kötve – akár fizető, akár nem fizető – előfizetők) számára érhető el, nem tesz magánjellegűvé egy ilyen hálózatot[18].

## 2.5 A „hozzáférés” fogalma – C.1. kritérium

27. A „hozzáférés” fogalmának helyes meghatározása érdekében fontos figyelembe venni az elektronikus hírközlési adatvédelmi irányelvnek az annak 1. cikkében meghatározott hatályát: *„az elektronikus hírközlési ágazatban a személyes adatok kezelése vonatkozásában az alapvető jogok és szabadságok védelm[e] egyenértékű szintjé[nek biztosítása] – különös tekintettel a magánélethez és a bizalmas adatkezeléshez való jogra –, valamint […] az ilyen adatoknak, az elektronikus hírközlő berendezéseknek és az elektronikus hírközlési szolgáltatásoknak a Közösségen belüli szabad mozgásá[nak biztosítása]”*.

28. Dióhéjban, az elektronikus hírközlési adatvédelmi irányelv a magánélet védelmét szolgáló jogi eszköz, amelynek célja a közlések titkosságának és az eszközök integritásának védelme. Az elektronikus hírközlési adatvédelmi irányelv (24) preambulumbekezdése egyértelművé teszi, hogy természetes személyek esetében a felhasználó végberendezése a felhasználó magánszférájának részét képezi, és az azon tárolt adatokhoz a felhasználó tudta nélkül való hozzáférés súlyosan sértheti a felhasználónak a magánélet tiszteletben tartásához való jogát.

29. Az elektronikus hírközlési adatvédelmi irányelv a jogi személyeket is védi[19]. Az elektronikus hírközlési adatvédelmi irányelv 5. cikkének (3) bekezdése értelmében vett „hozzáférés” fogalmát következésképpen úgy kell értelmezni, hogy biztosított legyen e jogok harmadik felek által elkövetett jogsértésekkel szembeni védelme.

[16] Az Európai Parlament és a Tanács (EU) 2018/1972 irányelve (2018. december 11.) az Európai Elektronikus Hírközlési Kódex létrehozásáról (átdolgozás) (EGT-vonatkozású szöveg), a 2. cikk 1. pontja.

[17] Például a késleltetéstűrő hálózati rendszerek összefüggésében, amelyek olyan „tárolási és továbbítási technikákat” alkalmaznak, mint például a Briar nyílt forráskódú projekt.

[18] A nyilvános hírközlő hálózatok azonosításának további elemzéséhez lásd a BEREC-nek a nyílt internetről szóló rendelet végrehajtásáról szóló iránymutatásait (BoR (20) 112).

[19] Az elektronikus hírközlési adatvédelmi irányelv (26) preambulumbekezdése, lásd a fenti 17. pontot.

30. Az adattárolás vagy a hozzáférés független műveletek is lehetnek, amelyeket független szervezetek végeznek. Az elektronikus hírközlési adatvédelmi irányelv 5. cikke (3) bekezdésének alkalmazhatóságához nem szükséges, hogy az adattárolás és a tárolt adatokhoz való hozzáférés egyaránt megvalósuljon.

31. Amint azt a 29. cikk szerinti munkacsoport 9/2014. sz. véleménye megállapítja: *„A »tárol vagy hozzáfér« szavak azt jelentik, hogy a tárolásnak és a hozzáférésnek nem kell ugyanazon közlés során megtörténnie, és azokat nem kell ugyanannak a félnek végrehajtania. Az egyik fél által tárolt információ (beleértve a felhasználó vagy az eszköz gyártója által tárolt adatokat), amihez később egy másik fél fér hozzá, ezért szintén az 5. cikk (3) bekezdése alá tartozik.”*[20] A „hozzáférés” fogalmának alkalmazhatósága következésképpen nem függ a végberendezésen lévő adatok eredetétől.

32. Amennyiben egy szervezet a végberendezésben tárolt adatokhoz való hozzáférésre irányuló lépéseket tesz, alkalmazni kell az elektronikus hírközlési adatvédelmi irányelv 5. cikkének (3) bekezdését. Ez általában azt jelenti, hogy a hozzáférő szervezetnek proaktívan konkrét utasításokat kell küldenie a végberendezésnek a kívánt adatok megszerzése érdekében. Ez a helyzet például a sütik esetében, amikor a hozzáférő szervezet arra utasítja a végberendezést, hogy proaktívan adatokat küldjön minden további hiperszöveg átviteli protokoll (hypertext transfer protocol, a továbbiakban: HTTP) hívásról.

33. Ugyanez a helyzet akkor is, ha a hozzáférő szervezet olyan szoftvert helyez el a felhasználó végberendezésén, amely tárolásra kerül, majd proaktívan hív egy alkalmazásprogramozási felület (application programming interface, a továbbiakban: API) végpontot a hálózaton keresztül. További példaként említhető a JavaScript kód, amelynek esetében a hozzáférő szervezet arra utasítja a felhasználó böngészőjét, hogy a kívánt adatokkal küldjön aszinkron kéréseket. Az ilyen hozzáférés egyértelműen az elektronikus hírközlési adatvédelmi irányelv 5. cikke (3) bekezdésének hatálya alá tartozik, mivel a hozzáférő szervezet kifejezetten utasítja a végberendezést az adatok elküldésére.

34. Egyes esetekben előfordulhat, hogy a végberendezést a kívánt adatok visszaküldésére utasító szervezet és az adatokat fogadó szervezet eltér egymástól. Ez a két szervezet közötti közös mechanizmus fennállásából és/vagy alkalmazásából eredhet. Az eszköznek a tárolt adatok elküldésére való utasítása (például egy olyan protokoll vagy SDK[21] használatával, amelynek révén proaktívan adatokat küld) lehetővé teszi a végberendezésbe történő behatolást, és ilyen hozzáférés esetén ezért alkalmazhatóvá válik az elektronikus hírközlési adatvédelmi irányelv 5. cikkének (3) bekezdése. Amint azt a 29. cikk szerinti munkacsoport 9/2014. sz. véleménye megjegyzi, ez lehet a helyzet akkor, ha egy weboldal egy nyomkövető pixel beillesztésével arra utasítja a végberendezést, hogy adatokat küldjön harmadik felek hirdetési szolgáltatásainak[22]. E felhasználási esetet részletesebben tárgyalja a 3.1. szakasz.

## 2.6 Az „adattárolás” és a „tárolt adatok” fogalma – C.2. kritérium

35. Az elektronikus hírközlési adatvédelmi irányelv 5. cikkének (3) bekezdése értelmében vett adattárolás adatoknak egy felhasználó vagy előfizető végberendezésének[23] részét képező fizikai elektronikus adathordozón történő elhelyezésére vonatkozik.

[20] A 29. cikk szerinti munkacsoport 9/2014. sz. véleménye, 8. o.
[21] Az SDK (software development kit [szoftverfejlesztő készlet]) az alkalmazásszoftverek létrehozásának megkönnyítése érdekében rendelkezésre bocsátott szoftverfejlesztő eszközök összessége.
[22] A 29. cikk szerinti munkacsoport 9/2014. sz. véleménye, 9. o.
[23] Meghatározását lásd ezen iránymutatás 2.3. szakaszában.

36. Az adatokat jellemzően nem az eszköz memóriájához egy másik fél által való közvetlen hozzáférés révén tárolják egy felhasználó vagy előfizető végberendezésében, hanem úgy, hogy a végberendezésen lévő szoftvert konkrét adatok előállítására utasítják. Az ilyen utasítások révén történő tárolást úgy kell tekinteni, hogy azt közvetlenül a másik fél kezdeményezte. Ez magában foglalja meglévő protokollok – például böngészősüti-tárolás –, valamint testre szabott szoftverek használatát, függetlenül attól, hogy ki hozta létre vagy telepítette a protokollokat vagy szoftvereket a végberendezésen.

37. Az elektronikus hírközlési adatvédelmi irányelv nem szab alsó vagy felső határt azt illetően, hogy az adatoknak mennyi ideig kell az adathordozón lenniük ahhoz, hogy tárolt adatoknak minősüljenek, sem pedig a tárolandó adatok mennyiségét illetően.

38. Hasonlóképpen, a „tárolás” fogalma nem függ attól, hogy milyen típusú adathordozón tárolják az adatokat. A jellemző példák közé tartoznak a merevlemezes meghajtók (hard disk drive, HDD), a szilárdtestmeghajtók (solid state drive, SSD), az elektromosan törölhető, programozható, csak olvasható memória (electrically-erasable programmable read-only memory, EEPROM) és a véletlen hozzáférésű memória (random-access memory, RAM), de az olyan kevésbé jellemző adathordozók, mint a mágneses szalag vagy a központi feldolgozó egység (central processing unit, CPU) gyorsítótára, szintén nincsenek kizárva az alkalmazási körből. Az adathordozó csatlakoztatható belül (például SATA csatlakozáson keresztül) vagy kívülről (például USB csatlakozáson keresztül).

39. A „tárolt adatok” fogalma a végberendezésen már meglévő adatokra vonatkozik ezen adatok forrásától vagy jellegétől függetlenül. Ez magában foglalja az elektronikus hírközlési adatvédelmi irányelv 5. cikkének (3) bekezdése értelmében vett, fent ismertetett (akár a később hozzáférő fél, akár másik harmadik fél általi) adattárolás minden eredményét. E fogalom magában foglalja továbbá az elektronikus hírközlési adatvédelmi irányelv 5. cikke (3) bekezdésének hatályán kívül eső adattárolási folyamatok eredményeit, például a végberendezésen maga a felhasználó vagy előfizető, illetve a hardvergyártó által történő tárolást (például a hálózati kártyák MAC-címei), a végberendezésbe beépített érzékelőket vagy a végberendezésen végrehajtott folyamatokat és programokat, amelyek adott esetben a tárolt adatoktól függő vagy azokból származó adatokat állítanak elő.

# 3 FELHASZNÁLÁSI ESETEK

40. Amint arra ezen iránymutatás bevezetése rámutatott[24], ezen iránymutatás nem elemzi az elektronikus hírközlési adatvédelmi irányelv 5. cikkének (3) bekezdésében előírt, az előzetes hozzájárulás beszerzésére vonatkozó kötelezettség alóli kivételek alkalmazását. Az Európai Adatvédelmi Testület emlékeztet arra, hogy az adattárolás vagy a tárolt adatokhoz való hozzáférés minden esetében meg kell vizsgálni, hogy szükség van-e előzetes hozzájárulásra, vagy alkalmazható-e az elektronikus hírközlési adatvédelmi irányelv 5. cikkének (3) bekezdése szerinti kivétel. Az olvasónak ezért e műszaki elemzéssel összefüggésben figyelembe kell vennie a felhasználási esetében alkalmazandó kivételeket.

41. Azon konkrét összefüggés sérelme nélkül, amelyben használhatók azok a műszaki kategóriák, amelyek szükségesek annak megállapításához, hogy alkalmazható-e az elektronikus hírközlési adatvédelmi irányelv 5. cikkének (3) bekezdése, nem kimerítő jelleggel azonosíthatók azon széles körben használt azonosítók és adatok tág kategóriái, amelyek esetében alkalmazható lehet az elektronikus hírközlési adatvédelmi irányelv 5. cikkének (3) bekezdése.

42. A hálózati kommunikáció általában egy rétegezett modellre támaszkodik, amely azonosítók használatát teszi szükségessé a kommunikáció megfelelő létrehozásának és végrehajtásának lehetővé

[24] Lásd a fenti 4. pontot.

tétele érdekében. Ezen azonosítók távoli szereplőkkel való közlése szoftveren keresztül, elfogadott kommunikációs protokollokat követve történik. A fent kifejtetteknek megfelelően az a körülmény, hogy a fogadó szervezet nem feltétlenül azonos az adatok küldésére utasítást adó szervezettel, nem zárja ki az elektronikus hírközlési adatvédelmi irányelv 5. cikke (3) bekezdésének alkalmazását. Ez érinthet útválasztási azonosítókat, például a végberendezés MAC- vagy IP-címét, de munkamenet-azonosítókat (SSRC, Websocket azonosító) vagy hitelesítési tokeneket is.

43. Az alkalmazási protokoll ugyanígy számos mechanizmust foglalhat magában kontextusadatok (például „elfogadás" mezőt vagy felhasználói ágenst tartalmazó HTTP fejléc), gyorsítótárazási mechanizmus (például ETag[25]) vagy más funkciók (például sütik vagy HSTS[26]) biztosítása érdekében. Még egyszer, az adatgyűjtés érdekében e mechanizmusokra való támaszkodás (például az ujjlenyomatvétel[27] vagy a forrásazonosítók nyomon követése összefüggésében) az elektronikus hírközlési adatvédelmi irányelv 5. cikke (3) bekezdésének alkalmazásához vezethet.

44. Másrészt léteznek olyan összefüggések, amelyekben a végberendezésben telepített helyi alkalmazások bizonyos adatokat szigorúan a végberendezésen belül használnak, mint például az okostelefonok rendszer API-jai esetében (hozzáférés a kamerához, mikrofonhoz, GPS érzékelőhöz, gyorsítóchiphez, rádióchiphez, helyi fájlokhoz, névjegyzékhez, azonosítókhoz stb.). Ez lehet a helyzet az olyan webböngészők esetében is, amelyek az eszközön belül tárolt vagy előállított adatokat kezelnek (például sütik, helyi tárhely, WebSQL vagy akár maguk a felhasználók által szolgáltatott adatok). Az ilyen adatok valamely alkalmazás általi felhasználása nem minősül az elektronikus hírközlési adatvédelmi irányelv 5. cikkének (3) bekezdése értelmében vett „tárolt adatokhoz való hozzáférésnek", amennyiben az adatok nem hagyják el az eszközt, de ha ezen adatokhoz vagy azok bármely származékához hozzáférés történik, alkalmazni kell az elektronikus hírközlési adatvédelmi irányelv 5. cikkének (3) bekezdését.

45. Végül egyes esetekben a szereplők rosszindulatú szoftverelemeket, például kriptobányászati szoftvereket vagy általánosabban kártékony szoftvereket helyeznek el, kihasználva a végberendezés feldolgozási képességeit az elhelyező szereplő javára. Az említett rosszindulatú szoftvereknek a felhasználó végberendezésén történő elhelyezése az elektronikus hírközlési adatvédelmi irányelv 5. cikkének (3) bekezdése értelmében vett „tárolásnak" minősül. Továbbá, ha a szoftver hálózati kapcsolatot hoz létre adatok későbbi küldése érdekében, az az elektronikus hírközlési adatvédelmi irányelv 5. cikkének (3) bekezdése értelmében vett „hozzáférésnek" minősül.

46. E kategóriák közül azok esetében, amelyek – akár széles körben elterjedt használatuk miatt, akár azért, mert használatuk körülményeire tekintettel külön vizsgálat indokolt – különleges érdeklődésre tartanak számot, az alábbiakban külön elemzés elvégzésére kerül sor.

## 3.1 URL-es és pixeles nyomon követés

47. A nyomkövető pixel egy forrásra mutató hiperlink, általában egy képfájl, amely be van ágyazva egy tartalomba, például egy weboldalba vagy egy e-mailbe. E pixel általában nem a kért tartalomhoz kapcsolódó célt szolgál; egyetlen célja, hogy automatikusan olyan kommunikációt hozzon létre a kliens és a pixel gazdája között, amelyre egyébként nem került volna sor. Ez azonban nem szisztematikus, és

[25] A HTTP ETag egy olyan azonosító, amely feltételes kérést tesz lehetővé a gyorsítótárazott kliensadatok érvényessége alapján.
[26] A szigorú HTTP biztonság (HTTP strict transport security, HSTS) lehetővé teszi a szerverek számára annak meghatározását, hogy mely forrásokat kell mindig HTTPS kapcsolatok használatával kérni.
[27] Amint azt a bevezetés megjegyezte, lásd a 29. cikk szerinti munkacsoportnak az elektronikus hírközlési adatvédelmi irányelvnek az eszköz-ujjlenyomatvételre való alkalmazásáról szóló 9/2014. számú véleményét.

nyomkövető pixelek úgy is létrehozhatók, hogy további információkat adnak hozzá a felhasználó számára megjelenített tartalomhoz kapcsolódó, hiperlinket betöltő képekhez. A kommunikáció létrehozása a konkrét felhasználási esettől függően különböző adatokat továbbít a pixel gazdájának.

48. E-mail esetében a feladó egy nyomkövető pixelt is elhelyezhet abban, hogy érzékelje, hogy a címzett mikor olvassa el az e-mailt. A weboldalakon elhelyezett nyomkövető pixelek olyan szervezettel hozhatnak létre kapcsolatot, amely számos ilyen kérést gyűjt össze, és így nyomon tudja követni a felhasználók magatartását. Az ilyen nyomkövető pixelek a link részeként további azonosítókat, metaadatokat vagy tartalmat is tartalmazhatnak. Ezen adatokat a weboldal tulajdonosa – adott esetben a felhasználó adott weboldalon végzett tevékenységéhez kapcsolódóan – összesítheti analitikai felhasználási jelentések létrehozása érdekében. Azok dinamikusan is létrehozhatók a szervezet által biztosított kliensoldali alkalmazási logika révén.

49. A nyomkövető linkek ugyanígy működhetnek, de az azonosító a weboldal címéhez van csatolva. Amikor a felhasználó meglátogatja az egységes forrás-helymeghatározót (uniform resource locator, a továbbiakban: URL), a célzott weboldal betölti a kért forrást, de egy olyan azonosítót is begyűjt, amely nem releváns a forrásazonosítás szempontjából. Ezeket igen gyakran használják az e-kereskedelmi weboldalak bejövő forgalomforrásuk eredetének azonosítására. Az ilyen weboldalak például nyomon követett linkeket biztosíthatnak partnereik számára a saját doménjükön történő használat érdekében, és így az e-kereskedelmi weboldal tudja, hogy melyik partnere felelős az eladásért, és melyik partnerének kell jutalékot fizetnie; ez a gyakorlat partnermarketing néven ismert.

50. Mind a nyomkövető linkek, mind a nyomkövető pixelek sokféle csatornán, például e-maileken, weboldalakon, vagy – a nyomkövető linkek esetében – akár bármilyen szöveges üzenetküldő rendszeren keresztül juttathatók célba. Ez a felhasználó végberendezéséhez történő eljuttatás tárolásnak minősül, legalábbis a kliensoldali szoftver gyorsítótárazási mechanizmusa révén. Az elektronikus hírközlési adatvédelmi irányelv 5. cikkének (3) bekezdése ennélfogva alkalmazandó, még ha ez a tárolás nem állandó jellegű is.

51. Nyomkövető információknak a felhasználónak küldött URL-ekhez vagy képekhez (pixelekhez) történő hozzáadása a végberendezésnek a kívánt adatok (a meghatározott azonosító) visszaküldésére adott utasítást jelent. A dinamikusan létrehozott nyomkövető pixelek esetében az utasítást az alkalmazási logika (általában egy JavaScript kód) elhelyezése képezi. Következésképpen úgy tekinthető, hogy az ilyen nyomonkövetési mechanizmusok révén biztosított azonosítók gyűjtése az elektronikus hírközlési adatvédelmi irányelv 5. cikkének (3) bekezdése értelmében vett „hozzáférésnek” minősül, így e rendelkezés erre a lépésre is alkalmazandó.

## 3.2 Helyi feldolgozás

52. Egyes technológiák a felhasználók végberendezésein elhelyezett szoftverek utasítására történő helyi feldolgozásra támaszkodnak, amelynek esetében a helyi feldolgozás által előállított adatokat a kliensoldali API-n keresztül elérhetővé teszik a kiválasztott szereplők számára. Ez lehet a helyzet például a webböngésző által biztosított API esetében, amikor a helyben generált eredmények távolról is hozzáférhetők.

53. Ha a feldolgozott adatokat bármely ponton és például a kliensoldali kódban hozzáférhetővé teszik egy harmadik fél számára, például a hálózaton keresztül visszaküldik egy szerverre, akkor az ilyen művelet (amelyre a felhasználó végberendezésén elhelyezett kliensoldali kódot előállító szervezet ad utasítást) „tárolt adatokhoz való hozzáférésnek” minősül. Az a körülmény, hogy ezen adatok előállítására helyben kerül sor, nem zárja ki az elektronikus hírközlési adatvédelmi irányelv 5. cikke (3) bekezdésének alkalmazását.

## 3.3 Kizárólag IP-n alapuló nyomon követés

54. Egyes szolgáltatók olyan megoldásokat dolgoznak ki, amelyek kizárólag egy elem, nevezetesen az IP-cím begyűjtésére támaszkodnak a felhasználó böngészésének – egyes esetekben több doménen keresztül történő – nyomon követése[28] érdekében. Ebben az összefüggésben az elektronikus hírközlési adatvédelmi irányelv 5. cikkének (3) bekezdése még akkor is alkalmazható lehet, ha az IP rendelkezésre bocsátására vonatkozó utasítást a fogadó szervezettől eltérő szervezet adta.

55. Az IP-címekhez való hozzáférés mindazonáltal csak abban az esetben teszi alkalmazhatóvá az elektronikus hírközlési adatvédelmi irányelv 5. cikkének (3) bekezdését, ha ez az adat egy előfizető vagy felhasználó végberendezéséből származik. Bár általában nem ez a helyzet (például a CGNAT[29] aktiválása esetén), a felhasználó útválasztójából származó statikus kimenő IPv4 ebbe az esetkörbe tartozik, ahogyan az IPV6-címek is, mivel azokat részben a gazda határozza meg. Kivéve, ha a szervezet biztosítani tudja, hogy az IP-cím ne egy felhasználó vagy előfizető végberendezéséről származzon, meg kell tennie az elektronikus hírközlési adatvédelmi irányelv 5. cikkének (3) bekezdése szerinti valamennyi lépést.

56. Bár ezen iránymutatás nem elemzi az elektronikus hírközlési adatvédelmi irányelv 5. cikkének (3) bekezdésében előírt, az előzetes hozzájárulás beszerzésére vonatkozó kötelezettség alóli kivételek alkalmazását, fontos ismételten emlékeztetni arra, hogy e cikk alkalmazhatósága nem jelenti szisztematikusan azt, hogy be kell szerezni az előzetes hozzájárulást. Az Európai Adatvédelmi Testület ezért emlékeztet arra, hogy minden egyes esetben meg kell vizsgálni, hogy szükség van-e előzetes hozzájárulásra, vagy alkalmazható-e az elektronikus hírközlési adatvédelmi irányelv 5. cikkének (3) bekezdése szerinti kivétel[30].

## 3.4 Időszakos és közvetített IoT jelentés

57. Az IoT (dolgok internete) eszközök időben folyamatosan szolgáltatnak adatokat például az eszközbe beépített érzékelők révén, amelyek helyben vagy előfeldolgozásra kerülnek, vagy nem. Sok esetben az adatokat elérhetővé teszik egy távoli szerver számára, de ezen adatgyűjtés módozatai eltérőek lehetnek.

58. Egyes IoT eszközök közvetlenül kapcsolódnak egy nyilvános hírközlő hálózathoz mobil SIM-kártya segítségével. Más eszközök közvetetten kapcsolódhatnak egy nyilvános hírközlő hálózathoz például WIFI használata vagy az adatoknak egy másik eszközre pont-pont összeköttetésen (például bluetooth-on) keresztül történő továbbítása révén. A másik eszköz lehet például okostelefon vagy egy célra rendelt átjáró, amely vagy előre feldolgozza az adatokat a szervernek történő megküldésük előtt, vagy nem.

59. Az IoT eszközöket a gyártó arra utasíthatja, hogy mindig streameljék az összegyűjtött adatokat, de először helyben gyorsítótárazzák azokat például a kapcsolat elérhetővé válásáig.

[28] Ez kiegészítő jellegű az IP-címnek az alapul szolgáló műszaki kommunikáció létrehozása és átvitele vagy továbbítása céljából történő használatához és e szempontból betöltött funkciójához képest, és független ezektől vagy azon körülménytől, hogy személyes adatnak minősül-e az vagy sem (az elektronikus hírközlési adatvédelmi szempontú elemzés szempontjából az „adatnak” minősül).

[29] A szolgáltatói szintű NAT-ot vagy CGNAT-ot az internetszolgáltatók a korlátozott IP-címterület maximális kihasználása érdekében használják. Az több előfizetőt tömörít ugyanazon nyilvános IP-cím alá.

[30] A 29. cikk szerinti munkacsoport 9/2014. sz. véleménye tartalmaz néhány példát arra az esetre, amikor nem feltétlenül van szükség előzetes hozzájárulásra.

60. Mindenesetre az IoT eszköz, amennyiben (közvetlenül vagy közvetve) egy nyilvános hírközlő hálózathoz kapcsolódik, maga is végberendezésnek minősül. Az a körülmény, hogy az adatokat streamingelik vagy gyorsítótárazzák az időszakos jelentésekhez, nem változtatja meg az adatok jellegét. Az elektronikus hírközlési adatvédelmi irányelv 5. cikkének (3) bekezdése mindkét esetben alkalmazandó, mivel az IoT eszközön található kód arra való utasítása révén, hogy a dinamikusan tárolt adatokat küldje a távoli szerverre, „hozzáférés” valósul meg.

## 3.5 Egyedi azonosító

61. Az „egyedi azonosítók” vagy „tartós azonosítók” a vállalatok által általánosan használt eszközök. Ilyen azonosítók a felhasználó eszközén hasított, tartós személyes adatokból (név és vezetéknév, e-mail cím, telefonszám stb.) származhatnak, és azokat több adatkezelő gyűjti és osztja meg egymással, hogy egyedileg azonosítsanak egy személyt különböző adatállományokban (weboldal vagy alkalmazás használata során gyűjtött felhasználási adatok, online vagy offline vásárláshoz vagy előfizetéshez kapcsolódó ügyfélkapcsolat-kezelési [CRM] adatok stb.). A weboldalakon általában hitelesítés vagy hírlevelekre való feliratkozás keretében szerzik meg a tartós személyes adatokat.

62. A fent kifejtetteknek megfelelően az a körülmény, hogy az adatokat a felhasználó adja meg, nem zárja ki az elektronikus hírközlési adatvédelmi irányelv 5. cikke (3) bekezdésének alkalmazását a tárolás tekintetében, mivel ezen adatokat begyűjtésük előtt ideiglenesen tárolják a végberendezésen.

63. Az „egyedi azonosítók” weboldalakon vagy mobilalkalmazásokon keresztül történő gyűjtésének összefüggésében az adatgyűjtő szervezet utasítja a böngészőt (a kliensoldali kód elhelyezése révén) az adatok elküldésére. Így „hozzáférés” valósul meg, és alkalmazni kell az elektronikus hírközlési adatvédelmi irányelv 5. cikkének (3) bekezdését.