

Az anonimizálás és az újraazonosítás aktuális kérdései, különös tekintettel a bírósági határozatok felismerhetetlenné tételére

SCHULTZ MÁRTON*

Az anonimizálás nem pusztán nevek és azonosítók kifejeztetését, kitakarását jelenti. Ezt mutatja az is, hogy mindannyian találkoztunk már olyan esetekkel, amikor egy személy minden ilyen anonimizálási törekvés ellenére továbbra is felismerhető maradt vagy néhány egyszerű internetes keresés után azzá vált. A jelen tanulmány az anonimizálás aktuális kérdéseit járja körül, különös figyelmet fordítva a személyes adat fogalmának relatív megközelítésével kapcsolatos uniós és magyar jogértelmezési tendenciákra, valamint az anonimizálás elhatárolására az álnevesítéstől. Az anonimizálással és a felismerhetetlenné tételrel kapcsolatos számos jó gyakorlatot mutatunk be, hogy mind a közhatalmi szervek, mind a magánszereplők gyakorlata optimalizálható legyen. Ezen belül elsősorban a bírósági határozatok közzétételének speciális szabályaira helyeződik a hangsúly, hiszen azok időbeli korlátozás nélkül, bárki számára hozzáférhetők. Kiemelten foglalkozunk a bírósági és a hatósági ügyszámok kérdéskörével, a közéleti szereplőkkel kapcsolatos döntések felismerhetetlenné tételével, azonban a legnagyobb hozadék a konkrét esetek jó és rossz gyakorlatainak összegyűjtése és bemutatása.

Kulcsszavak: adatvédelem, anonimizálás, felismerhetetlenné tétel, álnevesítés, bírósági határozatok

Current Issues of Anonymisation and Re-Identification, With Special Regard to the Rendering of Court Decisions Unrecognisable

Anonymisation is not just about rendering or blacking out names and identifiers. It is demonstrated by the fact that all of us have come across situations where, despite all these apparent efforts at anonymisation, a person has remained recognisable, or has become so after a few simple Internet searches. This paper outlines the current issues of anonymisation, paying particular attention to the trends in EU and Hungarian legal interpretation of the relative approach to the concept of personal data, as well as to the distinction between anonymisation and pseudonymisation. A number of good practices on anonymisation and non-disclosure will be presented in order to optimise the practices of both public authorities and private actors. In particular, the focus will be on the specific rules for the publication of judicial decisions, which are accessible to all without any limitation in time. The study also focuses on the issue of court and public authority case numbers, and the de-identification of public figures, however, its greatest contribution is the collection and presentation of good and bad practices in specific cases.

Keywords: data protection, anonymisation, rendering unrecognisable, pseudonymisation, court decisions

* Adatvédelmi tisztviselő, Szellemi Tulajdon Nemzeti Hivatala.

1. Bevezetés

A digitális technológiák segítségével az adatok, így a személyes adatok automatizált kezelése óriási méreteket ölt. Az Európai Bizottság felvázolt előrejelzése szerint 2025-re az előállított adatok mennyisége 175 zettabájtra nő.¹ Az adatokat sokszor aggregált, összesített módon, anonimizálva vagy az érintettre vonatkozó információktól megtisztítva, pszeudonimizáltan, álnevesítve (*hash-clve*) kezelik. Az üzleti szféra adatkezelését támogatandó, a 29. cikk szerinti munkacsoport (WP29) 2014-ben útmutatót adott ki az anonimizálási technikákról.² Azonban a közzétett adatok ezt nem tudja teljes mértékben hasznosítani, mert jellemzően más problémákkal szembesül az anonimizálással és a felismerhetetlenné tétellel összefüggésben, mivel az adatot hordozó iratok más jellegűek és struktúrájúak, mint a magánszféra adatkezeléseiben.

A Nemzeti Adatvédelmi és Információszabadság Hatóság (NAIH) 2013-ban ugyan kiadott egy útmutatót a védett adatot nem tartalmazó kivonatok készítéséhez, ez azonban elsősorban az ilyen adatokat tartalmazó iratok technikai megoldásaira fókuszált.³ A meg nem ismerhető adatok redaktálási módjairól, megismerhetetlenné tételének kérdéseiről viszont még nem született sem tanulmány, sem hatósági állásfoglalás vagy segédlet. A felismerhetetlenné tétellel kapcsolatos jogi problémák egyik fő területe a bírósági határozatok redaktálása. Ezt több tanulmány is vizsgálta összehasonlító jelleggel 2013-ban,⁴ szorosan kapcsolódva az Országos Bírósági Hivatal (OBH) által kezdeményezett igazságügyi adatkezeléssel kapcsolatos törvény – sikertelen – kodifikálásához.⁵ A bírósági határozatok nyilvánossága és közzététele a közérdekű adatok megismerésének egy sajátos területét képezi, ami az általánostól eltérő szabályanyagban is megnyilvánul. E terület viszonylag jól kutatható, vizsgálható, hiszen nagy számban áll rendelkezésre nyilvános határozat. Ugyanez kevésbé mondható el a hatósági határozatokról és más hatósági ügyiratokról, dokumentumokról, de a bírósági határozatokkal kapcsolatban azonosított problémakörök és jó gyakorlatok legnagyobb része ezek esetében is figyelembe vehető lehet.

A tanulmány középpontjában nem a bírósági határozatok nyilvánossága, hanem az azokban megjelenő felismerhetetlenné tételi módszerek, jó gyakorlatok állnak. Az anonimizálás és a felismerhetetlenné tétel fogalmának bemutatását követően kitérünk az anonimizálás és az álnevesítés viszonyára, ami mind a köz-, mind a magánszféra adatkezelését nagymértékben érinti. Ha ugyanis egy közzétett bírósági határozatot látszólag megfosztunk a személyes adatoktól, az érintettek mégis azonosíthatók maradnak, akkor legfeljebb álnevesítésről beszélhetünk, ami adatkezelésnek minősül. Ezt követően számos gyakorlati példán keresztül mutatjuk be az anonimizálási és a felismerhetetlenné tételi technikákat, ismertetve a bírósági határozatokra vo-

¹ A Bizottság közleménye az Európai Parlamentnek, a Tanácsnak, az Európai Gazdasági és Szociális Bizottságnak és a Régiók Bizottságának. Európai adatstratégia, COM(2020) 66 final.

² WP29 05/2014. számú vélemény az anonimizálási technikákról.

³ NAIH-1938-2/2013/T.

⁴ BALOGH Zsolt György: A bírósági határozatok közzétételének szabályozása Magyarországon. *Infokommunikáció és Jog*, 2013/2., 84.; GÖRÖG Márta: A bírósági ítéletek anonimizálásának gyakorlata a német és osztrák bírói fórumokon. *Infokommunikáció és Jog*, 2013/2., 81.; ZÓDI Zsolt: A bírósági határozatok és iratok nyilvánossága a *common law* egyes országaiban és az EU bíróságain. *Infokommunikáció és Jog*, 2013/2., 76.

⁵ Adatvédelmi és információszabadság-oldalról részletesen bemutatja a Nemzeti Adatvédelmi és Információszabadság Hatóság beszámolója a 2013. évi tevékenységéről, J/13824, 126–132.

natkozó speciális rendelkezéseket is. A tanulmányt három témakör vizsgálata zárja: az ügyszámok nyilvánossága, a közszereplők személyes adatainak törlése, valamint a személynevek törlése a megjelölésekkel kapcsolatos jogvitákban.

Célunk, hogy olyan jó gyakorlatokat gyűjtsünk össze az anonimizálás és a felismerhetetlenné tétel területén, amelyeket egyes információk meg nem ismerhetővé tétele során a közszféra szervezetei és magánszereplők is hasznosítani tudnak. Az erre vonatkozó jogirodalom és jogalkalmazási gyakorlat meglehetősen hiányos, külföldi példái is igen nehezen fellelhetők, és azok is csak általános szabályozási problémákkal foglalkoznak, amilyenekkel a magyar jogalkotás már korábban megbirkózott.⁶ A bemutatott elméleti és gyakorlati kérdések a nem gépi, hanem elsősorban a manuális megismerhetetlenné tételre vonatkoznak, és jellemzően egy-egy dokumentum, irat kis mennyiségű, emberi beavatkozást és értelmezést igénylő módosítása keretében értelmezhetők.

Korábbi kutatásokban vagy a napi munka során előkerülő, viszonylag friss, néhány éves jogesetek köréből hozzuk a példáinkat. Ebből a szempontból a tanulmány nem törekszik teljességre, csupán tipikus problémákat kíván azonosítani, remélve, hogy a bemutatott jó gyakorlatok megkönnyíthetik a közfeladatot ellátó szervek és más adatkezelők tevékenységét.

2. Az anonimizálás és a felismerhetetlenné tétel elhatárolása

2.1. Az anonimizálás

Az anonimizálást sem az általános adatvédelmi rendelet (GDPR),⁷ sem az információs önrendelkezési jogról és az információszabadságról szóló 2011. évi CXII. törvény (Infotv.) nem definiálja. Ugyanakkor a GDPR azokat az információkat tekinti anonimnak, amelyek „nem azonosított vagy azonosítható természetes személyre vonatkoznak, valamint az olyan személyes adatokra, amelyeket olyan módon anonimizáltak, amelynek következtében az érintett nem vagy többé nem azonosítható”.⁸ A nemzeti adatvagyon hasznosításának rendszeréről és az egyes szolgáltatásokról szóló 2023. évi CI. törvény (új Natv.) szerint az anonimizálás a személytelenítés körébe tartozó fogalom, és a személyes adatok olyan átalakítását jelenti, amelynek következtében az érintett többé nem azonosítható.⁹ Az új Natv. tehát bevezeti az uniós terminológiában ismeretlen személytelenítés fogalmát, amely alatt a személyhez kapcsoltság technikai megoldás-

⁶ Michal BOBEK: Data Protection, Anonymity and Courts. 26(2) *Maastricht Journal of European and Comparative Law* (2019), <https://doi.org/10.1177/1023263X19851628>, 183–189.; Edita GRUODYTÉ – Saulé MILČIUVIENĖ: Anonymization of Court Decisions in the EU: Actual and Comparative Issues. *Tėisės Apžvalga Law Review*, 2018/2., <https://doi.org/10.7220/2029-4239.18.3>, 60–70.; Edita GRUODYTĖ – Saulė MILČIUVIENĖ: Anonymization of Court Decisions: Are Restrictions on the Right to Information in „Accordance with the Law”? 9(2) *Baltic Journal of Law & Politics* (2016), <https://doi.org/10.1515/bjlp-2016-0016>, 150–170.

⁷ 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 rendelet hatályon kívül helyezéséről.

⁸ Uo. (26) preambulumbekzdés.

⁹ 2023. évi CI. törvény a nemzeti adatvagyon hasznosításának rendszeréről és az egyes szolgáltatásokról 2. § 6. pont.

sal való megszüntetését érti, ennek révén személytelenített adat jön létre (2. § 33. pont). A nyílt hozzáférésű adatokról szóló irányelv¹⁰ értelmében az anonimizálás egy dokumentum olyan anonim dokumentummá történő átalakítása, amely nem azonosított vagy azonosítható természetes személyre vonatkozik, valamint a személyes adatok olyan anonim adatokká történő átalakítása, amelyek alapján az érintett nem vagy többé nem azonosítható.

Látható tehát, hogy az anonimizálás túlterjeszkedik a szűkebb értelemben vett adatvédelem, és szorosan összefügg a közérdekű adatok megismerésével és terjesztésével, valamint az adatmegosztással. Az anonimizálás legnagyobb előnye, hogy az így létrejövő adatok lényegében nem lesznek személyes adatok, azokra az adatvédelmi szabályok többé nem vonatkoznak.¹¹ Tehát az anonimizált adatok kezelése a GDPR értelmében nem is minősül adatkezelésnek. Ennek különös jelentősége van a statisztikai és a kutatási célú adatkezelések esetén, de a hírközlési ágazatban is.¹²

Az új technológiák, mint a felhőalapú számítástechnika vagy a kvantumszámítógépek alkalmazása, esetleg az új információk birtokába jutás nagyban elősegítheti az anonimnek hitt adatok újraazonosíthatóságát. A közhiedelemmel ellentétben az anonimizálás az újraazonosítást nem szünteti meg, csupán egy meghatározott valószínűség alá csökkentheti,¹³ ezáltal megakadályozza egyes adatok összekapcsolását az érintettel, ahogyan azt is, hogy olyan következtetéseket lehessen levonni, amelyek révén az érintett azonosíthatóvá válik.¹⁴

2.2. A felismerhetetlenné tétel

Az Infotv. szerint felismerhetetlenné kell tenni egy másolaton a meg nem ismerhető adatot akkor, ha a közérdekű adatot tartalmazó dokumentum az igénylő által meg nem ismerhető adatot is tartalmaz [30. § (1) bekezdés]. A felismerhetetlenné tétel nemcsak a személyes adatokra, hanem minden meg nem ismerhető adatra vonatkozik. Ezek körét a jogszabályok nem határozzák meg, azt a bírói és a hatósági jogalkalmazási gyakorlat alakítja ki, csakúgy, mint azokat a módokat, amelyekkel az adatok meg nem ismerhetővé tehetők. Mivel személyes adat is minősülhet a nyilvánosság által meg nem ismerhető információnak, annak anonimizálása is felismerhetetlenné tételnek minősül, vagyis a felismerhetetlenné tétel tágabb fogalom. Az OBH szerint anonimizálás alatt a következőket kell érteni: „a dokumentumban az eljárással érintett személy azonosítását lehetővé tevő személyes és egyéb védett adatok eltávolítása vagy az azonosítást megakadályozó adatokra cserélése”,¹⁵ így azt lényegileg a felismerhetetlenné tétellel azonosítja.

¹⁰ Az Európai Parlament és a Tanács (EU) 2019/1024 irányelve (2019. június 20.) a nyílt hozzáférésű adatokról és a közszféra információinak további felhasználásáról 2. cikk 7. pont.

¹¹ GDPR (26) preambulumbekkezdés.

¹² 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 (26) preambulumbekkezdés, 6. cikk (1) bekezdés, 9 cikk (1) bekezdés.

¹³ Ten Misunderstandings Related to Anonimisation. AEPD-EDPS: <https://bit.ly/44Cc2po>.

¹⁴ WP29 05/2014. számú vélemény az anonimizálási technikákról, 10.

¹⁵ 4/2021. (III. 12.) OBH utasítás 3. § (1) bekezdés 1. pont.

Az információs szabadság területén az egyes adatok közzététele során az ún. adatelvnek megfelelően kell eljárni. Az állandó joggyakorlat szerint az egy dokumentumban, iratban található adatokat külön-külön kell vizsgálni, mert ezek egy része nyilvános, míg más része nem, és a nem nyilvános adatok is többféle szempont alapján minősülhetnek ilyennek, ennél fogva nem az egész iratot, hanem az egyes adatokat szükséges minősíteni.¹⁶ Fontos szabály, hogy a felismerhetetlenné tételt jellemzően annak a személynek kell elvégeznie, aki ismeri a dokumentumot, ezért tudja, mely adatok védettek és melyik adatból milyen további következtetést lehet levonni a peres felekre vagy más személyekre nézve.¹⁷ Finn kutatók szerint egy átlagos bírósági döntés anonimizálása 38 percet vesz igénybe, amiből 20 perc a döntés szövegével való megismerkedés.¹⁸

3. Az anonimizálás és az álnevesítés elhatárolása: a személyes adatok fogalmának relatív megközelítése

A GDPR szerint álnevesítésnek a személyes adatok olyan kezelése minősül, amelynek következtében további információk felhasználása nélkül többé már nem állapítható meg, hogy a személyes adat melyik konkrét természetes személyre vonatkozik. Révész Balázs szerint az ilyen adatkezelésnek az a lényege, hogy „a gyűjtött adatok és a természetes személy közötti kapcsolat csak egy külön tárolt kapcsolati kód alapján állítható helyre”.¹⁹ Az álnevesített adatok tehát személyes adatok, kezelésük pedig adatkezelés, azonban nem képeznek külön adattípust, csak egy speciális adatbiztonsági, technikai intézkedést jelentenek.²⁰

Az álnevesítés feltétele egyrészt az, hogy az azonosításhoz szükséges további információt külön tárolják, másrészt az, hogy megfelelő technikai és szervezési intézkedések megtételével biztosított legyen, hogy azonosított vagy azonosítható természetes személyekhez nem lehet hozzákapcsolni ezt a személyes adatot.²¹ Ez lecsökkenti az adatvédelmi kockázatokat,²² hiszen ha jogosulatlan személy csak az álnevesített adatokhoz fér hozzá, de a kiegészítő információkhoz nem (például a titkosítási kulcshoz), akkor nem lesz képes arra, hogy azokat az érintettekhez kapcsolja. Az anonimizálás során az adatkezelőnek minden olyan eszközt és módszert figyelembe kell vennie, amelyet harmadik személyek valószínűsíthetően felhasználhatnak az újraazonosításra.²³ Ehhez az összes objektív tényezőt figyelembe kell venni, így az azonosítás költségét és időigényét, valamint az adatkezeléskor rendelkezésre álló technológiát és annak fejlődését.²⁴

¹⁶ 3056/2015. (III. 31.) AB határozat; NAIH-4236/2022.

¹⁷ NAIH-1938-2/2013/T.

¹⁸ Minna TAMPER et al.: *Anonymization Service for Finnish Case Law: Opening Data Without Sacrificing Data Protection and Privacy of Citizens*. Paper presented at International Conference on Law via the Internet, Florence, Italy, 2018, 3.

¹⁹ RÉVÉSZ Balázs: 4. Alapfogalmak. In PÉTERFALVI Attila – RÉVÉSZ Balázs – BUZÁS Péter (szerk.): *Magyarázat a GDPR-ról*. Budapest, Wolters Kluwer, 2018, 86.

²⁰ CZAPÁRI Dóra – SZÓKE Gergely László: Az adatvédelem és az adathasznosítás egyik kulcskérdése: a személyes adatok anonimizálása. *JURA*, 2022/4., 32.

²¹ GDPR 4. cikk 5. pont.

²² GDPR (28) preambulumbekzdés, 32. cikk (1) bekezdés a) pont.

²³ WP 216, 3.

²⁴ GDPR (26) preambulumbekzdés.

A személyes adatok abszolút megközelítése értelmében egy információ személyesadat-jellege nem függ az adatkezelő személyétől, mivel az adatoknak az érintettre vonatkozása objektív, így akkor is adatkezelésről van szó, ha az adatkezelő maga nem, csupán más személy azonosíthatja az érintettet. Ezen belül különbséget lehet tenni aszerint, hogy egy másik adatkezelőnél vagy máshol található információ felhasználásával azonosítható-e egy természetes személy vagy sem.²⁵ A relatív megközelítés értelmében az a fontos, hogy a címzett, az adatkezelő szubjektíve össze tudja-e kapcsolni az adatot egy személlyel, vagyis hogy az érintettre vonatkozóan minősül-e az adat az ő tudása, ismeretei, valamint észszerű erőfeszítései alapján. A kérdéses adatok így egy bizonyos személy számára személyes adatoknak minősülhetnek, míg más személyek számára nem.

A joggyakorlatban több ügyben vizsgálták, hogy az adatkezelő vagy harmadik személy képes-e akár közvetett módon azonosítani az érintetteket. Az európai adatvédelmi biztos jogértelmezése és a Kúria korábbi gyakorlata szerint az anonimizált adatok bizonyos szempontú relatív értelmezése összeegyeztethető az adatvédelmi szabályokkal. Egyes kutatók azt javasolják, hogy a bírósági ítéleteket csupán álnevesíteni kellene, hogy az adatok a jövőben jobban hasznosíthatók legyenek.²⁶

Az Európai Unió Bírósága (EUB) a 2016-os Breyer-ügyben foglalkozott az IP-címek személyesadat-jellegével. A döntésben kimondta: az a tény, hogy az internetes honlap felhasználója azonosításához szükséges további adatokkal nem az elektronikus médiaszolgáltató, hanem a felhasználó internet-hozzáférést nyújtó szolgáltatója rendelkezik, nem zárja ki, hogy a dinamikus IP-címek személyes adatoknak minősüljenek.²⁷ A konkrét esetben az elektronikus médiaszolgáltató rendelkezett olyan módszerekkel, amelyek lehetővé tették az újraazonosítást az IP-cím alapján. Az EUB ugyanakkor rámutatott, hogy az újraazonosítás elsősorban akkor nem lehetséges, ha ahhoz aránytalan idő-, költség- vagy munkaráfordítás szükséges.²⁸

Az Európai Törvényszék egy friss ügyben kiemelte, hogy a címzett számára anonimnak kell tekinteni az álnevesített személyes adatokat akkor, ha a címzett további információk felhasználása nélkül nem tudja újraazonosítani az érintetteket, és ilyen információhoz jogszerűen nem is férhet hozzá. Ezt az adatkezelőnek az eset egyedi körülményeire tekintettel meg kell vizsgálnia.²⁹ A döntés nem a GDPR-ral kapcsolatban született, de a 2018/1725 rendelet³⁰ értelmezett fogalmai azzal azonosak. Hasonló döntést hozott a Kúria 2019-ben, szintén nem a GDPR-t értelmezve. A tényállás szerint álnevesített egészségügyi adatok esetén a titkosítási kulccsal nem rendelkező szervezeteknél lévő kódolt adatok nem minősülnek személyes

²⁵ CZAPÁRI–SZŐKE i. m. (20. lj.) 29.

²⁶ Gergely Márk CSÁNYI et al.: Challenges and Open Problems of Legal Document Anonymization. 13(8) *Symmetry* (2021), <https://doi.org/10.3390/sym13081490>, 25.

²⁷ C-582/14 Breyer [44].

²⁸ Uo. [46].

²⁹ T-557/20.

³⁰ Az Európai Parlament és a Tanács (EU) 2018/1725 rendelete (2018. október 23.) a természetes személyeknek a személyes adatok uniós intézmények, szervek, hivatalok és ügynökségek általi kezelése tekintetében való védelméről és az ilyen adatok szabad áramlásáról, valamint a 45/2001/EK rendelet és az 1247/2002/EK határozat hatályaon kívül helyezéséről.

adatnak, azokra nem vonatkozik az adatvédelmi szabályozás.³¹ A döntést bemutató Halász Bálint e kúriai jogértelmezéssel kapcsolatosan nem támasztott aggályt.³²

Hasonló kérdéssel foglalkozott a NAIH egy 2020-as ügyben, amelyben e kúriai határozat megállapításait is figyelembe vette. Az ügyben az érintettek az adatkezelő számára nem voltak közvetlenül azonosíthatók, azonban az álnevesített adatok átadása az adatkezelőnek éppen az érintettek azonosítását szolgálta,³³ így a NAIH szerint az ügyben a személyes adatok relatív megközelítése nem foghatott helyt. Pók László szerint a vizsgálat során elsősorban arra kell figyelemmel lenni, hogy az álnevesítéskor alkalmazott technikai eljárások révén az adatok elvesztik-e személyesadat-jellegüket, vagy ezek az eljárások csupán adatbiztonsági intézkedésnek minősülnek, és az adatok továbbra is egy azonosítható személyre vonatkoznak.³⁴

Az, hogy egy adatot anonimnak vagy csak álnevesítettnek tekintünk-e, mindig az eset körülményeitől függ. Álláspontunk szerint a GDPR kezdeti, szigorú védelmét egy rugalmasabb, kockázatalapú megközelítés váltja fel, így a személyes adat relatív megközelítése mindaddig támogatott, amíg az érintettek jogai és szabadságai kellő védelemben részesülhetnek.

4. Anonimizálási technikák

Két biztonságos anonimizálási technikát említ a 29. cikk szerinti munkacsoportnak a bevezetőben már hivatkozott véleménye: az általánosítást és a véletlenítést. A vélemény számos olyan informatikai, matematikai és statisztikai szempontból releváns tényezőt, eljárást tartalmaz, amely a manuális felismerhetetlenné tétel és az anonimizálás esetében nem releváns, így abból csupán az általánosítás és a véletlenítés fogalmát kívánjuk röviden bemutatni. Ezután kitérünk a munkacsoport által nem említett redaktálásra és a maszkolásra is mint az információszabadság területén általánosan alkalmazott anonimizálási és felismerhetetlenné tételi technikára.

4.1. Véletlenítés

Véletlenítés alatt azokat a technikákat kell érteni, amelyek az adat és az érintett közötti szoros kapcsolat eltávolítása érdekében az adatok valóságnak való megfelelését változtatják meg.³⁵ Ugyanis ha az adatok kellően bizonytalanná válnak, akkor azoknak az érintettel való összekapcsolása többé már nem lehetséges. A munkacsoport szerint a véletlenítés önmagában nem csökkenti az egyes rekordok (adatok) egyediségét, mert „minden rekord továbbra is egyetlen érin-

³¹ Kúria Pfv.20954/2018/6.

³² HALÁSZ Bálint: A Kúria megerősítette a személyes adatok fogalmának relatív megközelítését. *TwoBirdsIdeas*, 2019. november 27., <https://bit.ly/4adau68>.

³³ NAIH/2020/1839/10.

³⁴ PÓK László: Hozzáférési jog gyakorlása álnevesített adatok tekintetében. *GDPR – adatvédelem mindenkinek*, 2023. október 18., <https://bit.ly/44vtUSL>.

³⁵ WP29 05/2014. számú vélemény az anonimizálási technikákról, 13.

tettől fog származni, de védelmet nyújthat a következtetési támadások/kockázatok ellen, és az általánosítási technikákkal összekapcsolva erősebb adatvédelmi garanciákat biztosíthat”.³⁶

A munkacsoport a véletlenítést ennél konkrétan nem magyarázza meg, csupán arra mutat rá, hogy ezenfelül további technikák lehetnek szükségesek az érintett azonosításának megakadályozásához, például a zajhozzáadás. A munkacsoport példája a zajhozzáadásra: „ha egy egyén magasságát eredetileg a legközelebbi centiméterig mérték meg, az anonimizált adatállomány a magasságot csak +/-10 cm pontossággal tartalmazhatja”.³⁷ Ezt a megoldást javasolja a Gazdasági Versenyhivatal titokmentes iratváltozatok elkészítéséről szóló útmutatója³⁸ is a piaci részesedések, az egyéb relatív mutatók, valamint az abszolút adatok, például a vállalkozás éves árbevétele esetében. Az információszabadság területén ez a technika nem igazán bír relevanciával.

4.2. Általánosítás

Az általánosítás az adat olyan jellemzőjét veszi alapul, amely egy nagyobb absztrakciós szinten található; egyfajta *genus proximumot* (adatifajtát) kell keresni, amelyben a kérdéses adat jelenti a *differentia specificát*. Az anonimizáláshoz az adatfajtvával kell helyettesíteni az adatot. A 29. cikk szerinti munkacsoport szerint az általánosítás azt jelenti, hogy „az érintettek attribútumait általánosítják vagy felhívítják a vonatkozó skála vagy nagyságrend módosításával (pl. régió város helyett, hónap hét helyett)”.³⁹ Ide sorolható az a bíróságok szervezetéről és igazgatásáról szóló 2011. évi CLXI. törvény (Bsz.) 166. § (1) bekezdésében foglalt szabály is, amely szerint egyes személyeket az eljárásban betöltött szerepüknek (például alperes) megfelelően kell megjelölni. Ez ennél általánosabban az „adatifajta” szerinti megjelölésként fogalmazható meg, azonban önmagában ez a megoldás nem mindig vezet anonimításhoz, így jellemzően további technikai intézkedésre van szükség.

4.3. Törlés, redaktálás és maszkolás

A GDPR nem ismeri az adattörlés fogalmát. Az Infotv. értelmében az adattörlés az adat felismerhetetlenné tétele oly módon, hogy annak helyreállítása többé nem lehetséges (3. § 13. pont). Ezen belül a maszkolás az adat kitakarását jelenti, a redaktálás pedig az adat véletlenszerű vagy értelmezhetetlen karakterekkel való helyettesítését, vagy az adat törlésének jelzését. A brit adatvédelmi hatóság a minőségi adatok nyilvánvaló anonimizálási módjai között említi a személyek nevének redaktálását, valamint ide sorolja a videófelveteleken a személyek arcának kitakarása és a hangfelvetelek elektronikus eltorzítása mellett azt is, ha egy riportban szándékosan megvál-

³⁶ Uo.

³⁷ Uo.

³⁸ Tájékoztató az üzleti titokra vonatkozó nyilatkozatokról és a titokmentes iratok benyújtásáról. GHV, <https://bit.ly/3ydOuuL>, 8.

³⁹ WP29 05/2014. számú vélemény az anonimizálási technikákról, 19.

toztatják a helyeket és a neveket.⁴⁰ A redaktálás során az anonimizáló csak bizonyos személyes adatokat tesz megismerhetetlenné, így a többi adat elveszti személyes jellegét. Az adatkezelő jellemzően az anonimizálást követően is adatkezelő marad, mivel az irat a rendelkezésére áll anonimizálatlan, eredeti formájában is.⁴¹

Az ír adatvédelmi hatóság maszkolásnak nevezi a nyilvánvaló vagy a közvetlen személyes azonosítók eltávolítását, ami további intézkedés nélkül nagyon nagy valószínűséggel eredményezheti egy személy újraazonosítását, így ez nem minősül biztonságos anonimizálási technikának.⁴² Lothar Determann is kiemeli, hogy pusztán egyes személyazonosító adatok redaktálása nem feltétlenül gátja az azonosításnak, hiszen olyan adatok maradhatnak a dokumentumban, amelyek „lehetővé teszik a redaktálási folyamat visszafordítását (például cím, születési dátum/hely stb.)”.⁴³

5. A felismerhetetlenné tétel megvalósításának módszerei

5.1. A felismerhetetlenné tétel általános szabályai

A Tromsøi Egyezmény szerint minden felismerhetetlenné tételt egyértelműen jelezni kell (6. cikk 2. pont). Az Infotv.-ben sem ehhez hasonló rendelkezés, sem más releváns szabály nem található. A NAIH szerint „[e]gyértelműen jelezni kell, hogy honnan töröltek adatot, mert a védett adat észrevétlen, nyomtalan törlése éppúgy meghamisíthatja a szöveg értelmét, mint egy adat meghamisítása, vagy valótlan betoldása”.⁴⁴ A felismerhetetlenné tétel jellemzően általánosítás útján valósul meg egyrészt azért, hogy a szöveg összefüggései fenn tudjanak maradni (például maradjon alany a mondatban), másrészt pedig azért, mert ezzel a törölt adathoz kapcsolódó információk megtarthatók, amelyek szintén szükségesek a szöveg érthetősége és koherenciája szempontjából (például annak jelzése, hogy az eredeti szövegben egy e-mail-cím volt olvasható, vagy hogy az adott szövegrész az érintett havi keresetéről tartalmazott információt).

E két szempont mellett további fontos követelmény, alapelv az, hogy a szöveg eredeti arányait a közzétett, nyilvános szövegváltozatnak is tükröznie kell, mivel az is információt hordoz, hogy mekkora a meg nem ismerhető adatok terjedelme. A NAIH szerint az adatokat megismerők jogosultak megtudni azt is, hogy egy szót, egy sort, egy bekezdést vagy egy oldalt töröltek-e.⁴⁵ A felismerhetetlenné tétel módja az adathordozótól is függ, így a papíralapú iratok esetében egyes adatok nem cserélhetők le, ezért a meg nem ismerhető adatokat csak elfedni, kifeketíteni lehet (a szöveg arányai sokkal könnyebben megtarthatók). Ehhez nyújt segítséget a NAIH 2013-as útmutatója. A digitális iratok tartalmába az anonimizáló könnyebben beleyülhet, egyes adatokat kicserélhet benne, de közben figyelnie kell egyrészt arra, hogy a szöveg ará-

⁴⁰ Anonymisation: Managing Data Protection Risk Code of Practice. Information Commissioner's Office, <https://bit.ly/44A4bZ7>, 22.

⁴¹ Uo. 58–59.

⁴² Guidance on Anonimisation and Pseudonimisation. Data Protection Commission (Ireland), <https://bit.ly/3UAGpYm>, 12.

⁴³ Lothar DETERMANN: *Determann adatvédelmi jogi útmutatója*. Budapest, HVG-ORAC, 2020, 24–25.

⁴⁴ NAIH-1938-2/2013/T, 4. tanács.

⁴⁵ Uo., 5. tanács.

nyai megváltozhatnak, másrészt pedig arra, hogy egyértelműen jelezze, hol tér el a nyilvános iratváltozat az eredetitől.

5.2. Felismerhetetlenné tétel a Bszi. alapján

A Bszi. azt mondja ki, hogy a *Bírósági Határozatok Gyűjteményében* (BHGY) „közöttett határozatban szereplő személyek azonosítását lehetővé tevő adatokat olyan módon kell törölni, hogy az ne járjon a megállapított tényállás sérelmével. Egyebekben a határozatban szereplő egyes személyeket az eljárásban betöltött szerepüknek megfelelően kell megjelölni” [166. § (1) bekezdés]. Az Alkotmánybíróság ugyanezen szabályok alapján teszi közzé döntéseit saját közzétételi listájában (ügykeresőjében).⁴⁶ A közzétett határozatokban fel kell tüntetni a bíróság és a jogterület megnevezését, a határozat meghozatalának évét, a határozat sorszámát, valamint azokat a jogszabályhelyeket, amelyek alapján a bíróság a határozatot hozta [165. § (1)–(2) bekezdés]. A Kúria által közzétett határozat mellett fel kell tüntetni a határozat elvi tartalmát, ennek hiányában rövid tartalmát, valamint az alkalmazott jogszabályokat [163. § (1b) bekezdés]. Problémás, hogy az elvi és a rövid tartalmat nem kezelik külön sem a bíróságok, sem az OBH.⁴⁷

A Bszi. emellett bizonyos adatok nyilvánosságát is előírja. Ilyen a közfeladatot ellátó személy családi és utóneve és beosztása, ha az adott személy az eljárásban közfeladatának ellátásával összefüggésben vett részt, a meghatalmazottként eljáró ügyvéd vagy kamarai jogtanácsos, továbbá a védő neve, az egyesület vagy alapítvány neve, székhelye és képviselőjének neve, valamint a közérdekből nyilvános adatok [166. § (2) bekezdés]. Speciális rendelkezések találhatók a határozat közzétételének részbeni vagy egészbeni mellőzéséről is [166. § (4)–(5) bekezdés]. Külön kimondja a törvény azt is, hogy az ott előírtakon túl más változtatás nem hajtható végre a szövegen [166. § (6) bekezdés]. Hasonló szabály az Infotv.-ben is indokolt lenne, bár ez áttételesen következik abból, hogy csak a meg nem ismerhető adatokat lehet felismerhetetlenné tenni [30. § (1) bekezdés].

Az Ítélezést Támogató Rendszer (ITR) többek között a határozatok szerkesztésére és anonimizálására szolgál.⁴⁸ A vonatkozó 26/2019. (XI. 25.) OBH utasítás különbséget tesz automatikus és kézi anonimizálás között. Automatikus anonimizálás esetén az „anonimizáló a bírósági határozatszerkesztő részét képező anonimizáló programban a szereplő által felkínált, a program által automatikusan képzett és a felismert szövegegységekre felkínált csereszövegeket jóváhagyja, vagy szükség esetén azokat módosítja vagy törli”.⁴⁹ A szereplő nem más, mint „az informatikai alkalmazás által kínált vagy szabadon kialakított csereszöveg, amely az anonimizálandó adat módosítására szolgál”.⁵⁰ A kézi anonimizálás alatt pedig az anonimizáló program által fel nem ismert, de anonimizálandó szövegegységek anonimizáló általi lecserélését kell érteni.⁵¹

⁴⁶ 2011. évi CLI. törvény 44. § (2) bekezdés.

⁴⁷ A közzététel kritikáját lásd SCHULTZ Márton: A 2021. évben hozott szellemi tulajdon-jogi tárgyú bírósági határozatok számossága, elvi tartalma és rövid tartalma. *Iparjogvédelmi és Szerzői Jogi Szemle*, 2022/6., 83–84.

⁴⁸ 26/2019. (XI. 25.) OBH utasítás 3. § 10. pont.

⁴⁹ Uo. 12. § (1) bekezdés.

⁵⁰ Uo. 3. § 17. pont.

⁵¹ Uo. 12. § (1) bekezdés.

Ahogy Zódi Zsolt fogalmaz, az ilyen automatikus anonimizálási módszerek és az ezeket támogató programok jelentősen leegyszerűsítik az anonimizálás folyamatát.⁵² Sajnálatos módon nem áll rendelkezésre hasonló megoldás a közigazgatási iratok felismerhetetlenné tételére – ott a dokumentumok és az adatok különböző típusú és felépítésű iratokban, dokumentumokban található meg, számos esetben csak papíron, nem pedig elektronikus formában, ezért nehezen képzelhető el automatikus anonimizálásra alkalmas program használata. A közigazgatási hatóságok nem olyan nagy számban teszik közzé határozataikat, mint a bíróságok, így valószínűsíthetően e területen sincs szándéka egy szervnek ilyen programra beruházni, hiszen az néhány határozat közzététele miatt nem éri meg a hatóságoknak.

5.3. A felismerhetetlenné tétel általánosítással

Míg a bíróságok esetében a főszabály az általánosítás mint anonimizációs technika, addig a közfeladatot ellátó más szervek esetében az Infotv. nem ír elő ilyen megkötést. A Bszi. szabályát, amely szerint a határozatban szereplő személyek neve helyett az eljárásban betöltött szerepüknek megfelelő elnevezést kell alkalmazni [166. § (1) bekezdés], az OBH utasítás – erre vonatkozó konkrét törvényi szabály hiányában – azzal egészíti ki, hogy „a személyek azonosítására szolgáló és a védett adatok helyett az adatfajta elnevezését” kell helyettesítő szöveggént alkalmazni.⁵³ Az általánosítás mint felismerhetetlenné tételi technika tehát nemcsak a személyek nevére, hanem valamennyi személyes adatra vonatkoztatandó. Ebből az is következik, hogy a közigazgatási határozatok felismerhetetlenné tétele más módon is elvégezhető, mert ezen a területen hasonló ágazati szabályozás nem ismert.

A bíróságok a bírósági határozathoz csatolt, közzétett hatósági határozatot is ezen a módon teszik felismerhetetlenné annak ellenére, hogy erre sem található szabály a Bszi.-ben. Ez felveti annak a veszélyét, hogy egy közzétett határozatot eltérő szövegváltozattal tesz közzé a bíróság és a hatóság, ami nem tűnik tudatos jogalkotói lépésnek. A jogi szövegekben, így a közigazgatási határozatokban is, sokszor elegendő a redaktálás, mert a szöveget eleve úgy fogalmazták meg, hogy egyes adatokat már az anonimizálás előtt általánosítják. Az általánosítás a jogi szövegekben elterjedt módszer, a felismerhetetlenné tétel kívánalmától függetlenül is.

Kötelezettséget erre vonatkozóan csupán a jogszabályok szerkesztésénél találhatunk. A vonatkozó miniszteri rendelet kimondja, hogy „ha a jogszabály tervezetének a szövegében ismétlődően valamely kifejezés, szókapcsolat, szövegrész fordul elő, az ismétlődő elem helyett rövid megjelölést lehet alkalmazni”.⁵⁴ Ezt kiegészíti azzal, hogy „a rövid megjelölést a rövidíteni kívánt elem első előfordulásakor kell meghatározni, és a további használatra utaló »a továbbiakban:« kifejezéssel együtt, zárójelben kell feltüntetni”.⁵⁵ Remek példa erre a következő szöveg: „A Nemzeti Adatvédelmi és Információszabadság Hatóság (a továbbiakban: Hatóság) [...] (laccíme: [...]); a továbbiakban: Kérelmező) a Hatósághoz 2022. július 25. napján érkezett ké-

⁵² ZÓDI Zsolt: A bíróságok és a technológia. *Bírósági Szemle*, 2020/1., 9.

⁵³ 26/2019. (XI. 25.) OBH utasítás 4. § (2) bekezdés.

⁵⁴ 61/2009. (XII. 14.) IRM rendelet 5. § (1) bekezdés.

⁵⁵ Uo. 5. § (2) bekezdés.

relmére, a [...] (lakcíme: [...]; a továbbiakban: Kérelmezett) által telepített kamerákkal összefüggő adatkezelés vizsgálatára indult adatvédelmi hatósági eljárásban az alábbi döntéseket hozza.⁵⁶ E példában a kérelmező neve (az első kipontozott adat) törléssel meg nem ismerhetővé tehető, mert maga az eredeti szöveg felelteti meg a kérelmező nevét a „kérelmező” szóval („a továbbiakban: Kérelmező”), így az általánosítás a szöveg többi része vonatkozásában már alapértelmezetten el van végezve. Ez a szövegszerkesztési és fogalmazási technika nagy könnyebbség az anonimizálónak is.

5.3.1. Az eljárásban betöltött szerepnek megfelelő megjelölés

A BHGY-ban közzétett határozatokban szereplő személyek sok esetben nem az eljárásban betöltött szerepüknek megfelelő elnevezést kapnak, hanem a monogramjukkal jelölik őket. Ez nem megfelelő gyakorlat, hiszen egyrészt nem felel meg a fent idézett jogszabálynak, másrészt nagyobb mértékben teszi lehetővé az újraazonosítást. Remek példa erre a gyakorlatra a Kúria által anonimizált alábbi határozatrészlet: „a tűzfalal kapcsolatos problémára K.Zs. tanú magyarázatot adott.”⁵⁷ Ilyen esetekben a „[tanú1]” vagy a „[tanú1 neve]” a megfelelő helyettesítő kifejezés.

A bíróság itt a tanú neve esetében a monogramra alakítás módszerét választotta, azonban a legtöbb – itt nem idézett – adatot redaktálta, így több megoldást alkalmazott egyszerre. Azt is érdemes kiemelni, hogy a redaktálást a „(…)” jellel oldotta meg, tehát nem szögletes, hanem ke-rek zárójellel. Célszerű lenne a szögletes zárójel alkalmazását állandósítani, bár úgy tűnik, nagyobb probléma az, hogy nem az adatfajta megjelölésével helyettesítik a törölt adatokat. Álláspontunk szerint vagy a szabályozáson kellene változtatni, mert az a gyakorlatban életszerűtlennek bizonyul, vagy pedig a tudatosság növelésére volna szükség az OBH és a NAIH részéről, hogy az anonimizálók megfelelő módon tegyék felismerhetetlenné az adatokat. A vonatkozó OBH utasítás értelmében a bírósági anonimizáló program az ún. szereplapon felkínált, a program által automatikusan képzett és a felismert szövegegyeségekre csereszöveget ajánl fel,⁵⁸ így ennek a formátuma is megváltoztatható, megváltoztatandó a megfelelő adatfajta.

5.3.2. Az adatfajta megjelölése

Az OBH a védett adatok esetében azt követeli meg, hogy az adatfajta jelöljék meg a közzétett határozatban, így például az üzleti titok, a banktitok, a minősített adat vagy a védett ismeret kifejezés szerepeljen a tényleges adattartalom helyett. Eddig nemigen lehetett találkozni ilyen szövegezésű határozattal. Szabadalmi ügyekben például a határozatban szereplő rajzot sok esetben törlik a közzétett iratváltozatban, anélkül, hogy jeleznék, hogy az eredeti határozatban ott egy rajz szerepelt.

Lényeges könnyebbséget jelent a bírósági anonimizálónak, hogy csak az adatfajta kell feltüntetnie, hiszen a közigazgatási információszabadság területén a korlátozás okát is meg kell jelölni. A Kúria szerint nem elegendő az üzleti titokra vagy *know-how*-ra mint megtagadási okra

⁵⁶ NAIH-6479-11/2022.

⁵⁷ Kúria Kfv.37033/2020/4.

⁵⁸ 26/2019. (XI. 25.) OBH utasítás 12. § (1) bekezdés.

minden konkrétum nélkül, általánosan hivatkozni, vagyis az adatkezelőnek meg kellene jelölnie, hogy az melyik szerződés melyik részében, milyen okból képez üzleti titkot (például egy cég nem nyilvános értékesítési mutatója), és ezt igazolnia is kell.⁵⁹ Az OBH utasítás szerint a személyek azonosítására szolgáló minden adat esetében az adatfajta kell behelyettesíteni,⁶⁰ így például a születési dátumok, az e-mail- és a lakcímek helyett is.

5.3.3. Ugyanazon adatfajta megjelölése azonos módon

Ugyanazt az adatot azonos formában kell felismerhetetlenné tenni a nyilvánosságnak szánt dokumentumban. Példaként hozható, hogy egy, a NAIH által közzétett határozatban egy internetes hivatkozást háromféleképpen redaktált a hatóság, így nem egyértelmű, hogy egy honlapról van-e szó vagy három különbözőről („https://www.....”, „www.....hu”, „Cikk link”).⁶¹ A döntésben három helyen találhatunk weboldalra mutató hiperlinket, három különböző formában. Ez alapján nem egyértelmű, hogy itt ténylegesen három vagy egy hivatkozásról van-e szó (esetleg csak kettőről). Általános szabály tehát, hogy ugyanazt az adatot a közzétett dokumentumban azonos formában kell megjeleníteni.

5.4. Felismerhetlenné tétel redaktálással

Bizonyos esetekben az adat vagy nem helyettesíthető mással, például a papíralapú iratok esetében, vagy a felismerhetlenné tétellel érintett adatok tartalma, tulajdonságai irrelevánsak. Ilyenkor nem más adattal vagy általánosítással, hanem törléssel vagy redaktálással kerül sor a felismerhetlenné tételre, ami többféleképpen valósulhat meg: szögletes zárójellel: „[...]”, kerek zárójellel: „(...)”, kipontozással: „...”, feketén kihúzott szöveggel: „■”, vagy az adatok félkövérre állításával is. Az osztrák adatvédelmi hatóság csillaggal (*) helyettesíti a redaktált szavakat, jellemzően ugyanannyi jellel minden szót, függetlenül azok hosszától. Ez a megoldás álláspontunk szerint olyan ügyszámok, lajstromszámok, azonosítószámok, pénzüsszegek megadásánál alkalmazandó, amelyek személyes adatnak vagy más védett információnak minősülnek. Ilyenkor, ha a körülményekből más nem következik, a karakterszám az eredetivel azonos is lehetne.

Amikor nem csupán töröljük vagy redaktáljuk az adatot, hanem helyettesítjük is valamivel, például az érintettre a neve helyett felperesként hivatkozunk, szintén érdemes lehet jelezni valamilyen módon, például a szövegrész vastagításával, hogy a szövegen változtatást hajtottak végre. Javasolt a szögletes zárójel használata ebben az esetben is, hiszen az köztudomásúan azt jelöli, hogy olyan szöveget illesztenek bele, amelyet az eredeti szöveg nem tartalmazott. Több módszer együttesen is alkalmazható, ha az indokolt (például számadatok esetén törlés helyett a karakterek helyettesítése * jellel).

⁵⁹ Kúria Pfv.20.733/2017/7.

⁶⁰ 26/2019. (XI. 25.) OBH utasítás 4. § (2) bekezdés.

⁶¹ NAIH-2853-1/2022.

6. Ügyszámok anonimizálása

6.1. A bírósági határozatok saját ügyszámai mint közérdekű adatok

A bírósági ügyszám az OBH szerint „az ügy azonosítására szolgáló megjelölés, amely tartalmazza az ügycsoport betűjelét, a lajstromszámot, törve az érkezés évszámával”.⁶² A bírósági határozatok ügyszámainak megismerhetőségével az Alkotmánybíróság 2019-ben foglalkozott. Az alapügy tényállása szerint a felperes azt kérte, hogy küldjék meg neki a folyamatban lévő olyan polgári peres eljárások listáját, amelyekben mind a felperesek, mind az alperesek jogi személyek, és az eljárás legalább hét éve tart. Az Alkotmánybíróság jogértelmezése tehát egyedi adatigényléssel és nem a bíróságok kötelező közzétételével függött össze, így az nem a BHGY-ba feltöltött határozatokban található ügyszámokkal volt kapcsolatos. Döntésében a testület rámutatott, hogy az ügyirat száma nem személyes adat, és az a bíróság közfeladatának ellátásával összefüggésben keletkezik.⁶³ Hasonló álláspontot fogalmazott meg a NAIH elnöke is az eljárás-hoz csatolt véleményében.⁶⁴ Kontextustól függően a bírósági határozatok ügyszámai minősülhetnek személyes adatnak, ezt mindig az egyedi eset körülményei alapján kell elbírálni.

Ki lehet jelenteni azt is, hogy a bírósági határozatok saját ügyszámai közérdekű adatnak minősülnek, és ezért azokat nem szükséges redaktálni a közzétett bírósági határozatokban. Különösképpen azért, mert ez alapján lehet azonosítani egy-egy ügyet, hivatkozni rá a joggyakorlatban, így ez hozzájárul a jogbiztonsághoz és az egységes joggyakorlathoz is. Gyakran lehet találkozni olyan, a BHGY-ban is közzétett határozattal, amely a bírósági ügyszámát annak ellenére nem tartalmazza, hogy a letöltött fájl neve azzal egyébként megegyezik. Ezen a rossz gyakorlaton mindenképpen változtatni kellene, hiszen így egy-egy döntés nem feltétlenül használható fel és terjeszthető ügy, ahogy arra szükség lenne.

A probléma természetesen ennél komplexebb: a bírósági döntések jellemzően nem csupán saját ügyszámmal rendelkeznek, hanem indoklásukban korábbi bírósági döntésekre is hivatkoznak, valamint az eljárás korábbi szakaszai bírósági és hatósági döntéseinek ügyszámát is tartalmazzák. Sajnálatos módon az anonimizálók sok esetben ezeket is törlik, így ezeket a döntéseket nem lehet külön megkeresni a BHGY-ban, így az azokban foglalt állítások nem ellenőrizhetők.

Az ügyiratszámok felismerhetetlenné tételei gyakorlatának nem egységes voltát remekül szemlélteti két véletlenszerűen kiválasztott védjegyjogi döntés. Az elsőnél a Fővárosi Ítéltábla által közzétett határozat tartalmazza a döntés saját ügyiratszámát, a korábban eljáró Fővárosi Törvényszék döntésének ügyszámát, és egy korábbi, az ügyhöz, de nem a pertörténethez kapcsolódó fővárosi ítéltáblai döntés ügyszámát. A Szellemi Tulajdon Nemzeti Hivatala releváns határozatai közül azonban csak az egyik ügyszám látható teljes terjedelemben, a másikat részben redaktálták, de ennek oka nem állapítható meg.⁶⁵ A másik, szintén a Fővárosi Ítéltábla által hozott, közel azonos időben közzétett döntés semmilyen ügyszámot nem tartalmaz, még a

⁶² 17/2014. (XII. 23.) OBH utasítás 3. § 38. pont.

⁶³ 13/2019. (IV. 8.) AB határozat.

⁶⁴ NAIH/2017/2409/2/V.

⁶⁵ Fővárosi Ítéltábla 8.Pkf.25.172/2021/3.

saját döntését sem.⁶⁶ Ha csak nyomtatott formában áll rendelkezésre a döntés, akkor az ügyszámra további információ felhasználása nélkül nem található meg.⁶⁷

6.2. Kapcsolódó korábbi hatósági ügyszámok hivatkozása

A Kúria is foglalkozott a döntéshez kapcsolódó korábbi közigazgatási döntések ügyszámokkal való hivatkozásával. Az ügy tárgya ráadásul a NAIH által az egyik határozatában megvalósított adatvédelmi incidens volt. A perbeli NAIH-határozat a felperes által indított adatvédelmi vizsgálati és hatósági ügyek számának és tárgyának megjelölését tartalmazta, valamint azt is, hogy az alperesnek hivatalos tudomása volt arról, hogy nála a felperes az alperesi érdekelttel szemben 13 adatvédelmi eljárást kezdeményezett, 13 különböző ügyszámon. A NAIH a határozatban négy további eljárás ügyszámát is feltüntette.

A Kúria a felülvizsgálati eljárás során rámutatott, hogy az ügyszámok annyiban minősülnek személyes adatnak, amennyiben azok lekérhetőek, és az ellenérdekű félnek a felperes ismeretében lehetősége van az ő személyének összekötésére az anonimizált döntések tartalmával, olyan esetekben is, amikor az anonimizált döntés nem tartalmaz az érdekeltre kiható rendelkezést. E döntés elvi tartalma szerint az eset körülményeitől függően adatvédelmi incidensnek minősülhet a félhez köthető azonos tárgyú ügyeik ügyszámmal való felsorolása a közigazgatási határozatban, ha azok az ügybeli jogviszonyokhoz nem kapcsolódnak.⁶⁸

7. Az érintettek azonosíthatósága bizonyos ügytípusokban

7.1. A személyes adatok nyilvánossága általában

A GDPR lehetőséget ad a tagállamoknak, hogy a személyes adatok védelmét összeegyeztessék a közérdekű adatok megismeréséhez való joggal (86. cikk), ideértve a bírósági határozatok és a közigazgatási ügyiratok nyilvánosságát is. E tagállami szabályozásokról a Bizottságnak nincs ismerete. Magyarországon az Infotv. értelmében *törvény* minősíthet egy személyes adatot közérdekből nyilvánossá (3. § 6. pont). Az Infotv. szerint az ilyen személyes adatok a célhoz kötött adatkezelés elvének betartásával szabadon terjeszthetők [26. § (2) bekezdés]. Ugyanakkor az információszabadság területén a cél nehezen azonosítható, hiszen az így megismerhető adatokat a kommunikációs alapjogok gyakorlásával összefüggésben bárki szabadon, bármilyen célra felhasználhatja.

E szabályt töri át a Bszi. a bírósági határozatok nyilvánosságra hozatalával összefüggésben, amikor kimondja, hogy a BHGY-ben közzétett határozatban szereplő személyek azonosítását

⁶⁶ Fővárosi Ítéltábla Pkf.25779/2020/3.

⁶⁷ Kivéve azt az esetet, amikor a döntés olyan speciális szavakat tartalmaz, amelyeket a szabad szöveges keresőbe beírva rábukkanhatunk a döntésre. Ez azonban lényegesen körülményesebb, mint az ügyiratszám megadása, különösen mert az éppen erre szolgál.

⁶⁸ Kúria Kfv.IV.37.361/2021/10.

lehetővé tevő adatokat olyan módon kell törölni, hogy az ne járjon a megállapított tényállás sérelmével [166. § (1) bekezdés]. Tehát a bírósági határozatoknál a jogalkotó a bírósági jogalkalmazóra, az anonimizálóra bízta azt, hogy a konkrét esetben döntsön arról, melyik adat szükséges a határozat tényállásának értelmezéséhez, így melyik személyes adatot nem szükséges felismerhetetlenné tenni. Ez azonban csupán azt meghaladóan érvényesülhet, hogy az eljárásban betöltött szerepüknek megfelelően jelölik meg az egyes személyeket, valamint a személyek azonosítására szolgáló és a védett adatok helyett az adatfajta elnevezését alkalmazzák helyettesítő szöveggént.⁶⁹ Az angolszász jogtudomány ezzel szemben hagyományosan nem törli a peres felek nevét és a más perben részt vevők nevét sem az ítéletekből. Zódi hívja fel a figyelmet arra, hogy az Egyesült Államokban a jogesetgyűjteményekhez csatolt névmutatókkal a perben részt vevő bármelyik személy neve alapján kereshetővé teszik a döntéseket.⁷⁰

7.2. A közéleti szereplők személyes adatai

Görög Márta hívja fel a figyelmet arra, hogy Németországban az abszolút kortörténeti szereplők nevét nem anonimizálják, mert ott a közönség tájékoztatáshoz való joga erősebb az információs önrendelkezési jognál.⁷¹ Így például a híres Marlene Dietrich-döntésben sem a művésznő, sem a felperesként fellépő lánya (Maria Riva) nevét nem anonimizálták. A döntés arra is kitért, hogy milyen volt az elhunyt színésznő magánélete, milyen mértékben vonult vissza a nyilvánosságtól és ez hogyan kapcsolódott a jogsértéshez.⁷² A német gyakorlat ezt kifejezett törvényi szabályozás hiányában teszi.

Hasonló megoldás üdvözlendő lenne Magyarországon is, hiszen számos esetben így válik ismertté egy-egy közszereplő ügye, a döntés mégis „anonim” marad. Fontos körülmény az is, hogy a tényállás szempontjából nemcsak a közéleti szereplés körülményeinek körülírása, hanem a közszereplőre vonatkozó adatok ismerete is fontos lehet a tényállás megértése szempontjából, amennyiben azok nem vonatkoznak az érintett magánéletére, emberi méltóságára. Balogh Zsolt már 2013-ban javasolta a közéleti szereplők nevének nyilvánosságra hozatalát a bírósági határozatokban, azok fokozottabb tűrési kötelezettségére hivatkozva.⁷³ Álláspontjához mi is csatlakozunk.

Mivel nagymértékben függ a konkrét eset körülményeitől, hogy a közszereplő magánélete mennyiben lehet érintett a közéleti kérdéseket, közügyeket is tárgyaló bírósági döntésben, véleményünk szerint általánosságban nem minősíthető közérdekből nyilvánossá a közéleti szereplők neve és más személyes adata. Egyes személyes adatok nyilvánossága szükséges a közéleti vitákhoz, sőt a sajtó társadalmi kontrollfunkciójának ellátásához is, ez azonban csak akkor lehet arányos, ha az a közéleti szereplő emberi méltóságát, magán- és családi életéhez való jogát nem sérti.

Az eljáró bíró, illetve tanács feladata lehetne annak eldöntése, hogy a közszereplő melyik személyes adatát nem szükséges felismerhetetlenné tenni a döntésben a konkrét eset és a tényál-

⁶⁹ 26/2019. (XI. 25.) OBH utasítás 4. § (2) bekezdés.

⁷⁰ ZÓDI i. m. (4. lj.) 77.

⁷¹ GÖRÖG i. m. (4. lj.) 81.

⁷² NJW 2000, 2195.

⁷³ BALOGH i. m. (4. lj.) 89.

lás figyelembevételével. Ezt a Bszi.-ben lehetne előírni, az a Bszi. 166. § (1) bekezdésének közéleti szereplőkre vonatkozó konkretizálása lehetne. Alkotmányellenes helyzetet eredményezne az, ha a technikai feladatot ellátó bírósági anonimizáló ítélne meg, hogy melyik személyes adat nem függ össze a közügyek vitatásával, mivel ezáltal a cél eléréséhez képest aránytalan mértékben korlátoznák a nyilvánosságot. Ennek okán álláspontunk szerint a bírór mérlegelését nélkülöző törvényi nyilvánossági szabály alapjog-korlátozó helyzetekhez vezethet a gyakorlatban, ami jogellenes adatkezeléssel is járhat.

A tényleges gyakorlat is ilyen – alkotmányos szempontból igazolható – irányt követel. Több olyan határozat van, amelyet a jogász szakma és a sajtó meghatározott személyekkel köt össze az anonimizálás ellenére is. Ilyen például a Görög Zita meztelen képeivel kapcsolatos döntés,⁷⁴ de az Alkotmánybíróságnak a kivételes közszereplő fogalmát kidolgozó döntése is, amelyet a „Hajdu–Puzsér-vitaként” ismertté vált ügyben hozott.⁷⁵ E döntésekben az anonimizálás következtében a személyek nem azonosíthatók, semmi nem utal arra, hogy azokban tényleg rólu- luk lenne szó. Más esetekben a döntésből az érintett azonosíthatóvá válik. Így például Gyurcsány Ferenc korábbi miniszterelnök egyértelműen azonosíthatóvá válik a Kúria döntésének szövegéből: „az a felperes miniszterelnöki tevékenységével összefüggésben, az ún. őszi beszé- det követő eseményekre...”⁷⁶ Szintén azonosíthatóvá teszi az anonimizált döntés tényállása Or- bán Ráheldt, akit a határozat „Magyarország miniszterelnökének lánya” megnevezéssel említ.⁷⁷ Más jellemzők, akár egy személyre jellemző mondat is azonosíthatja az érintettet, így például a „Jó estét, jó szurkolást!” idősebb Knézy Jenő sportújságíró.⁷⁸

7.3. Felismerhetetlenné tétel, ha a jogvita tárgya személynévvel függ össze

Bizonyos esetekben, különösen védjegyügyekben, de versenyjogi (jellegbitorlási) és személyiségi jogi ügyekben is, egy személy neve egyben más jogtárgy (például védjegy, domén- vagy kereskedelmi név) formáját is felveheti. Ilyen például Pick Jenő,⁷⁹ Herz Ármin,⁸⁰ Láng László⁸¹ neve is, amelyeket a közzétett döntésekben nem redaktáltak. Ezekben az esetekben a név ismereté- nek kulcsfontosságú szerepe lehet a tényállás megismerésében és az adott jogtárgyra (amely jel- lemzően ún. *szóbeli* megjelölés) vonatkozó joggyakorlat fejlesztésében, más esetektől való elkül- önítésében, hiszen a döntés a nevet fonetikailag, konceptuálisan és vizuálisan is vizsgálhatja. A közéleti szereplőkkel összefüggő más ügyekben nem magának a névnek, hanem a néven ke- resztül a személy azonosításának, a konkrét személyiségnek az ismerete bírhat relevanciával. Mi- vel minden közéleti szereplő egyéniség, egyedi tulajdonságokkal rendelkezik, más-más lehet a megítélésük, valamint a kontextus is, ami nagyban befolyásolhatja a döntést. Sok esetben a sajtó

⁷⁴ BDT2007. 171.

⁷⁵ Ab: Puzsér nevezhette pszichopátának Hajdu Pétert. *HVG*, 2018. április 25., <https://bit.ly/4dopFwa>.

⁷⁶ Kúria Pfv.IV.21.276/2015/5.

⁷⁷ Kúria Pfv.IV.20.908/2020/6.

⁷⁸ BH2002. 261.

⁷⁹ BH1997. 467.

⁸⁰ BH1993. 350.

⁸¹ Legfelsőbb Bíróság Pf. IV.21007/1992.

is beszámol ezekről az esetekről az érintettek nevének feltüntetésével, így a döntések anonimizálása inkább megnehezíti a társadalmi-jogi viták rekonstruálását és a kutatást.

Azok a döntések, amelyekben az érintettek a felismerhetetlenné tétel ellenére azonosíthatók maradnak, nem minősülnek anonimnak. A Polgári törvénykönyv rendelkezésének értelmében a közügyek szabad vitatását biztosító alapjogok gyakorlása a közéleti szereplő személyiségi jogainak védelmét szükséges és arányos mértékben, az emberi méltóság sérelme nélkül korlátozhatja. Az ilyen joggyakorlás azonban nem járhat a magán- és a családi élet vagy az otthon sérelmével.⁸² E rendelkezést konkretizáló szabályt a Bszi. nem tartalmaz. A korábbiakban kifejtetteknek megfelelően az is elképzelhető, hogy az eljáró bíróság – egyértelmű törvényi szabályozás híján – a döntésben rendelkezzen arról, hogy a közéleti szereplő melyik személyes adatát nem szükséges felismerhetetlenné tenni a közügyek vitatásával összefüggő, nem kizárólagosan magánéleti érintettségű ügyekben.

8. Következtetések

Mind az anonimizálás, mind a felismerhetetlenné tétel számos gyakorlati problémát vet fel. Az előbbi esetben a jogalkalmazási gyakorlaton múlik majd, hogy mit tekint még adatkezelésnek és így álnevesítést célzó technikai intézkedéseknek, valamint hogy mennyire enged a piaci igényeknek és szempontoknak az adatalanyok jogaival és jogos érdekeivel szemben. A utóbbi esetben úgy tűnik, hogy szükség van bizonyos mértékű jogegységesítésre, általános iránymutatásokra, különösen ami a bírósági és a hatósági határozatok közzétételét érinti. Ez nagymértékben hozzájárulhatna a bírósági anonimizálók tudatosságának növeléséhez és az egy-egy gyakorlathoz, emellett a magánszereplőket is segíthetné.

A NAIH 2013-as útmutatóján kívül semmilyen fogódzót nem ad a közfeladatot ellátó szervezetek az iratok redaktálásáról. Célszerű lenne ennek főbb szempontjait és módjait egységesíteni. Álláspontunk szerint nem elsősorban a jogszabályi környezet megváltoztatására van szükség, hanem a NAIH-nak és az OBH-nak kellene olyan iránymutatást kiadnia, amely mind az igazságszolgáltatás, a bíróságok, mind a hatósági, közigazgatási szervek felismerhetetlenné tételi gyakorlatát egységesíti azáltal, hogy a jogi szabályozás szintjét el nem érő bizonyos kérdésben állást foglal. Ilyen lehet az, hogy a redaktálás során az elektronikus dokumentumban törölt szöveg esetén szögletes zárójellel kell jelezni a törlést vagy új szöveg beillesztését, de akár az is, hogy védjegyügyekben a személynevet tartalmazó védjegyszót vagy lajstromozni kívánt megjelölést nem szabad törölni. E jó gyakorlatokra vonatkozó egységesítési törekvés megalapozhatná, előkészíthetné akár azt is, hogy a jövőben egységes nyilvános adatbázisba kerüljön a különböző közigazgatási szervek, a bíróságok és az Alkotmánybíróság joggyakorlata. Az anonimizálók iránymutatásokkal való ellátása növelné a tudatosságukat is, így jobban elkerülhető lenne bizonyos személyek újraazonosíthatósága is.

Az Infotv. kiegészítése több szempontból releváns lehet, így a felismerhetetlenné tétellel összefüggésben az anonimizálás szó szerepeltetése, valamint az, hogy a felismerhetetlenné tételt

⁸² 2013. évi V. törvény a Polgári Törvénykönyvről 2:44. § (1) bekezdés.

egyértelműen jelezni szükséges. Ilyen továbbá az is, hogy a meg nem ismerhető adatok felismerhetetlenné tételén túl az iraton más változtatás nem végezhető. A Bszi. mintájára a természetes személyek adataival összefüggésben célszerű lenne az Infotv.-ben olyan szabályt is elhelyezni, amely előírja, hogy az eljárásban érintett személyeket eljárási szerepüknek megfelelően kell megjelölni.

Ezt meghaladóan üdvözlendő lenne a NAIH, az OBH és a bíróságok fokozottabb együttműködése, valamint az esetlegesen felmerülő jogértelmezési problémák kezelése akár állásfoglalás, akár jogszabályváltoztatás útján. Meglátásunk szerint ez különösen is így van, mert a közigazgatási szervek nem igazán fordulnak a NAIH-hoz a felismerhetetlenné tétellel kapcsolatos problémákkal, így az ő tevékenységük csak a jogellenes adatkezelésekkel összefüggésben kerül a figyelem középpontjába. Mivel az ő esetükben a bírósági határozatok nyilvánosságához hasonló problémák jelentkeznek, az e területen kialakított megoldások sok esetben rájuk is alkalmazhatók lennének.

Irodalomjegyzék

- BALOGH Zsolt György: A bírósági határozatok közzétételének szabályozása Magyarországon. *Infokommunikáció és Jog*, 2013/2., 84–89.
- BOBEK, Michal: Data Protection, Anonymity and Courts. 26(2) *Maastricht Journal of European and Comparative Law* (2019) 183–189.
<https://doi.org/10.1177/1023263X19851628>
- CZAPÁRI Dóra – SZŐKE Gergely László: Az adatvédelem és az adathasznosítás egyik kulcskérdése: a személyes adatok anonimizálása. *JURA*, 2022/4., 24–48.
- CSÁNYI, Gergely Márk et al.: Challenges and Open Problems of Legal Document Anonymization. 13(8) *Symmetry* (2021).
<https://doi.org/10.3390/sym13081490>
- DETERMANN, Lothar: *Determann adatvédelmi jogi útmutatója*. Budapest, HVG-ORAC, 2020.
- GÖRÖG Márta: A bírósági ítéletek anonimizálásának gyakorlata a német és osztrák bírói fórumokon. *Infokommunikáció és Jog*, 2013/2., 81–84.
- GRUODYTÉ, Edita – MILČIUVIENĚ, Saulė: Anonymization of Court Decisions: Are Restrictions on the Right to Information in „Accordance with the Law”? 9(2) *Baltic Journal of Law & Politics* (2016) 150–170.
<https://doi.org/10.1515/bjlp-2016-0016>
- GRUODYTÉ, Edita – MILČIUVIENĚ, Saulė: Anonymization of Court Decisions in the EU: Actual and Comparative Issues. *Tėisės Apžvalga Law Review*, 2018/2., 60–70.
<https://doi.org/10.7220/2029-4239.18.3>
- HALÁSZ Bálint: A Kúria megerősítette a személyes adatok fogalmának relatív megközelítését. *TwoBirdsIdeas*, 2019. november 27., <https://bit.ly/4adau68>.
- PÓK László: Hozzáférési jog gyakorlása álnevesített adatok tekintetében. *GDPR – adatvédelem mindenkinek*, 2023. október 18., <https://bit.ly/44vtUSL>.
- RÉVÉSZ Balázs: 4. Alapfogalmak. In PÉTERFALVI Attila – RÉVÉSZ Balázs – BUZÁS Péter (szerk.): *Magyarázat a GDPR-ról*. Budapest, Wolters Kluwer, 2018, 63–94.

SCHULTZ Márton: A 2021. évben hozott szellemi tulajdon-jogi tárgyú bírósági határozatok számossága, elvi tartalma és rövid tartalma. *Iparjogvédelmi és Szerzői Jogi Szemle*, 2022/6., 76–108.

TAMPER, Minna et al.: *Anonymization Service for Finnish Case Law: Opening Data Without Sacrificing Data Protection and Privacy of Citizens*. Paper presented at International Conference on Law via the Internet, Florence, Italy, 2018.

ZÓDI Zsolt: A bírósági határozatok és iratok nyilvánossága a *common law* egyes országaiban és az EU bíróságain. *Infokommunikáció és Jog*, 2013/2., 76–80.

ZÓDI Zsolt: A bíróságok és a technológia. *Bírósági Szemle*, 2020/1., 4–13.

Elindítottuk a Jogkódex webböngésző alatt működő, bárki számára hozzáférhető, ingyenes változatát.

Próbálja ki a Jogkódexet!



jogkodex.hu

Már az ingyenes, bárki által elérhető verzióban is teljeskörűen megismerhetők az egyes §-okhoz kapcsolódó

- ▶ bírósági iránymutatások,
- ▶ más jogszabályi és alkotmánybírósági rendelkezések.

Emellett betekinthesz a §-okhoz kapcsolódó

- ▶ precedensekbe, döntvényekbe, anonim bírósági határozatokba,
- ▶ folyóirat szócikkekbe.

Használja mobiltelefonján és táblagépen is!

