

Az adatvédelem és az online szolgáltatások kapcsolódási pontjai

A digitális reziliencia és az értelmezési elsődlegesség sajátosságai

GOMBOS KATALIN*

A szolgáltatások nyújtása és igénybevétele az információs társadalom keretei között főként az online térben zajlik. Ezért felértékelődött annak szerepe, hogy a felügyeleti hatóságok (és végső soron a bíróságok) milyen módon jogosultak személyes adataink védelmére. A digitális rezilienciának nagy hatása van a 21. századi jogalkalmazói tevékenységre, amelyet az adatvédelem és az online szolgáltatások találkozási pontjai miatt szükségképpen a versengő jogok összemérése jellemez. Az uniós jog alkalmazása általánosságban is a tagállami jogoktól részben eltérő szemléletű jogértelmezési gyakorlatot kíván meg, de az adatvédelmi szemléletű jogalkalmazás ezen belül is sajátosságokat mutat. A felügyeleti hatóságok tevékenysége egyre inkább hangsúlyossá válik, és az Európai Unió Bíróságának esetjoga alapján jól látható a jogvédelmi célú jogalkalmazás szükségessége. A tendenciák alapján igazolható az értelmezési elsődlegesség e jogterületre eső néhány sajátossága is.

Kulcsszavak: információs társadalom, adatvédelem, digitális reziliencia, értelmezési elsődlegesség

The links between data protection and online services

The specificities of digital resilience and interpretive primacy

The supply and demand of services in the information society takes place mainly in the online space. The role of the supervisory authorities' (and ultimately the courts') powers to protect our personal data has therefore become more important. Digital resilience has a major impact on twenty-first century jurisdictional activity, which is necessarily characterised by a confrontation of competing rights at the intersection of privacy and online services. Even in general, the application of European Union law requires a partially different approach to the interpretation of national law, however, data protection law has its own specificities. The activity of supervisory authorities is becoming increasingly pronounced, and the need for a law enforcement approach with a view to protecting rights is clearly evident from the case law of the Court of Justice of the European Union. The trends also justify some of the specificities of interpretive primacy in this area of law.

Keywords: information society, data protection, digital resilience, interpretive primacy

* Egyetemi tanár, Nemzeti Közszolgálati Egyetem Államtudományi és Nemzetközi Tanulmányok Kar. ORCID-azonosító: 0000-0002-1014-0547.

1. Bevezetés

A szolgáltatásnyújtás szabadsága a négy uniós alapszabadság egyike.¹ Ennek egy jól azonosítható, egyre jelentősebb szerepet játszó területe az információs társadalommal függ össze. Általában a szolgáltatások kulcsfontosságúak az Európai Unió (EU) belüli üzleti és szakmai mobilitás szempontjából, a digitalizáció előretörésével pedig egyre több online szolgáltatás nyújtására és igénybevételére kerül sor. Manapság Európában ötödik alapszabadságként kezdik emlegetni az adatok (ezzel párhuzamosan a digitális kor új aranya, az adatvagyon) szabad mozgásának – és erre vonatkozóan az EU bármely országában minden uniós polgár számára ugyanolyan szintű jogvédelem – megteremtését. Az online térben nyújtott és igénybe vett szolgáltatások esetében kiemelkedő jelentősége van az adatvédelem biztosíthatóságának, ezért a két jogterület találkozása miatt az Európai Unió Bíróságának (EUB) egyrészt egyre többször kell versengő jogokat összemérnie, ennek keretében a személyes adatokhoz való jog és az információs társadalommal összefüggő jogok kapcsolódási pontjait megítélve, másrészt gyakran kell autonóm uniós jogi fogalmakat értelmeznie, de legalábbis uniós jogforrásokban szereplő fogalmak értelmezési tartományát uniós módszertannal meghatározni. Fontos kiindulópont az is, hogy az európai integrációban az autonóm jogrendszerként létező uniós jognak² – amelynek a normái alkotta jogrend különbözik mind a nemzetközi jogtól, mind a tagállamok belső jogrendjétől³ – saját jogi terminológiája, autonóm jogi fogalomhasználata és önálló értelmezési módszertana van,⁴ ezért az EUB által adott jogértelmezés különös jelentőségű.

Az uniós joggal kapcsolatban általánosan kimondható, hogy autonóm fogalmi rendszerrel dolgozik, ezért egy irányelv esetében – különösen a közvetlen vagy közvetett hatály doktrínájának alkalmazási kötelezettsége, egy rendelet esetében pedig már a közvetlen alkalmazhatóság miatt – a tagállami jogalkalmazóknak is az autonóm fogalmakat kell használniuk saját jogalkalmazási tevékenységük során. Ez akár azt is jelentheti, hogy el kell vonatkoztatni a tagállami fogalmi keretektől, és egy uniós jogforrásban használt – akár a tagállami jogokban is előforduló – fogalmakhoz uniós jogi tartalmat kell társítani, azaz korántsem biztos, hogy a tagállami jogi fogalmak kellően elkalauzolnak bennünket az uniós jog világában is.⁵

Nyitott jogalkalmazói gondolkodásra lehet szükség, amelynek az egyik fő jellemzője az, hogy az összehasonlító módszereknek is teret enged,⁶ és az uniós jogforrásban adott fogalommeghatározó norma híján az egyes tagállamok közös vagy éppen egyedileg sajátos jogi

¹ Lásd részletesebben Catherine BARNARD: *The Substantive Law of the EU: The Four Freedoms*. Oxford, Oxford University Press, 2022, <https://doi.org/10.1093/he/9780192857880.001.0001>, 37–197.

² Eredeti megfogalmazásában: közösségi jog. Lásd a Bíróság 1991. december 14-i 1/91. számú véleményét.

³ VÖRÖS Imre: Európai jog – magyar jog: konkurencia vagy koezisztencia? *Jogtudományi Közöny*, 2011/7–8, 369–401.

⁴ Koen LENAERTS – José Antonio GUTIÉRREZ-FONS: *Les méthodes d'interprétation de la Cour de justice de l'Union européenne*. Brussels, Bruylant, 2020; Koen LENAERTS – José Antonio GUTIÉRREZ-FONS: *Az Európai Unió Bíróságának jogértelmezési módszerei* (ford. LUKÁCS Adrienn, ORBÁN Endre, SIMON Emese Réka). Budapest, HVG-ORAC, 2022, 36–39.

⁵ C-443/03 Leffler [45]–[46].

⁶ Lásd Mads ANDENAS – Duncan FAIRGRIEVE: *Courts and Comparative Law*. Oxford, Oxford University Press, 2015, <https://doi.org/10.1093/acprof:oso/9780198735335.001.0001>, 117–232; C-119/05 Lucchini.

hagyományai adhatnak támpontot egy értelmezendő uniós fogalom valós értelmének behatárolására.⁷ Ennek egyik lehetséges módja az uniós jog többnyelvűségéből levezethető, különböző nyelvi változatok szerinti értelmezés.⁸ Ezeken túl értelmezési alap lehet az alapszerződés,⁹ jogelvek,¹⁰ a „precedensek”,¹¹ a nemzetközi szerződések,¹² az alapjogok,¹³ a tagállamok közös alkotmányos hagyományai,¹⁴ az erkölcsi értékek,¹⁵ a közös jogi hagyományok¹⁶ és a szokások¹⁷ fényében való interpretáció is. A fogalmak tartalmának helyes megállapításához gyakran több módszer együttes alkalmazására és komplex értelmezésre van szükség.¹⁸

A fenti – valamennyi uniós jogterület értelmezésénél irányadó – módszertan mellett különös jelentősége van az adatvédelmi jog és az online szolgáltatásnyújtás szabadsága találkozási pontjait jellemző digitalizációs sajátosságnak, továbbá annak is, hogy a jogok érvényesülését garantáló szabályok betartatásában felügyeleti hatóságok működnek közre, így e hatóságok jogkörei tényleges érvényesülésében, határainak megvonásában kulcsfontosságúak lehetnek a digitális térben újszerű problémaként jelentkező jogértelmezési kérdések. Kiinduló hipotézisünk az, hogy a 21. századi hatósági tevékenység legalább akkora részben (főként digitális adatokkal kapcsolatos) jogvédelmi jellegű jogalkalmazás, mint amekkora részben szabályozó hatósági feladatok ellátását célzó, témánk szempontjából elsősorban (piac)felügyelet.

A vázolt jogértelmezési és jogvédelmi tendenciák gyakorlatát az EUB újabb esetjoga alapján vizsgáljuk, amihez az EU által 2016 májusában elfogadott adatvédelmi csomag keretében született két legfontosabb jogforrás, az általános adatvédelmi rendelet (GDPR)¹⁹ és a bűnüldö-

⁷ C-119/05 Lucchini.

⁸ C-29/69 Stauder kontra Stadt Ulm.

⁹ C-218/82 Bizottság kontra Tanács [15]; C-201/85 és C-202/85 Klensch kontra Secrétaire d'État egyesített ügyek [21]; C-314/89 Rauh kontra Hauptzollamt Nürnberg-Fürth [17]; C-98/91 Herbrink kontra Minister van Landbouw, Natuurbeheer en Visserij; C-1/02 Borgmann [30].

¹⁰ C-418/97 és C-419/97 Vereniging Dorpsbelang Hees és társai egyesített ügyek [37].

¹¹ A C-389/05 Bizottság kontra Franciaország ügyben 2008. július 17-én hozott ítéletben a Bizottság érvelése egy korábbi „ítélet fényében” megfogalmazást tartalmazta. Példaként hozható az az eset is, hogy amikor a Bizottság versenyfelügyeleti jogkörében határozatot hoz, amely megtámadható a Törvényszék és – jogkérdés tekintetében utóbb – az EUB előtt is, gyakran már a határozata megfogalmazásából is kitűnik a bíróságok „vezérdöntéseinek” figyelembevétele.

¹² C-344/04 IATA és ELFAA [35].

¹³ C-311/04 Algemene Scheeps Agentuur Dordrecht [25]; C-61/94 Bizottság kontra Németország [52]; C-286/02 Bellio Flli [33].

¹⁴ Az Európai Unióról szóló szerződés 6. cikk.

¹⁵ C-275/92 H.M. Customs and Excise kontra Schindler [58]; C-124/97 Läärás és társai [33].

¹⁶ C-36/02 Omega [36]; C-438/05 The International Transport Workers' Federation és The Finnish Seamen's Union [75].

¹⁷ T-222/99, T-327/99 és T-329/99 Bonino és társai kontra Parlament egyesített ügyek.

¹⁸ C-283/81 CILFIT kontra Ministero della Sanità.

¹⁹ 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 (általános adatvédelmi rendelet).

zésben érvényesítendő adatvédelemről szóló irányelv,²⁰ továbbá az információs társadalom²¹ szolgáltatásaival összefüggésben a médiaszolgáltatások nyújtására vonatkozó audiovizuális médiaszolgáltatásokról szóló irányelv²² egyes rendelkezéseit – és a versengő jogok közötti eligazodáshoz az EU Alapjogi Chartájának releváns rendelkezéseit – használjuk fel.

2. A felügyeleti hatóságok jogköreit értelmező bírói gyakorlat jelentősége

Az EUB joggyakorlatában fontos szerepet töltenek be az online szolgáltatásokat nyújtók feletti felügyeletet gyakorló hatóságok feladatainak értelmezésével kapcsolatos ügyek. Ebben a körben az úttörő szerepet a Schrems-ügyek játszották, amelyekben az EUB a személyes adatok harmadik országbeli adatfeldolgozóknak való továbbítása kérdéseit vizsgálta. A GDPR azt a főszabályt tartalmazza, hogy az ilyen adatok csak akkor továbbíthatók valamely harmadik országba, ha az ezen adatok számára megfelelő védelmi szintet biztosít.²³ Azt, hogy a belföldi jog vagy a nemzetközi kötelezettségek alapján megfelel-e a követelménynek az adott harmadik ország védelmi szintje, a Bizottság jogosult megfelelőségi határozatában megállapítani. Enélkül az adattovábbítás csak akkor teljesíthető, ha egyrészt a személyes adatoknak az EU-ban letelepedett átadója megfelelő garanciákat nyújt, másrészt ha hatékony jogvédelem áll az érintett személyek rendelkezésére, különösen jogaik érvényesíthetőségére és a jogorvoslati eszközök igénybevételének lehetőségére vonatkozóan.

2.1. Fókuszban az általános adatvédelmi rendelet – a kezdeti lépések

Az Ausztriában lakóhellyel rendelkező, osztrák állampolgárságú, 2008 óta Facebook-felhasználó Maximillian Schrems személyes adatait a Facebook Ireland részben vagy egészben a Facebook Inc. Egyesült Államokban található szervereire továbbította és azokat ott kezelték.

²⁰ Az Európai Parlament és a Tanács (EU) 2016/680 irányelve (2016. április 27.) a személyes adatoknak az illetékes hatóságok által a bűncselekmények megelőzése, nyomozása, felderítése, a vádeljárás lefolytatása vagy büntetőjogi szankciók végrehajtása céljából végzett kezelése tekintetében a természetes személyek védelméről és az ilyen adatok szabad áramlásáról, valamint a 2008/977/IB tanácsi kerethatározat hatályon kívül helyezéséről.

²¹ Jelentőségéről lásd VÁRADI Szilvia: Az információs társadalom iránti bizalom erősítését célzó szabályozási módszerek az uniós adatvédelem területén. In STRIHÓ Krisztina – SZEGEDI László (szerk.): *Európai szabályozáspolitikai kihívások*. Budapest, Ludovika, 2022, 195–204.

²² Az Európai Parlament és a Tanács 2010/13/EU irányelve (2010. március 10.) a tagállamok audiovizuális médiaszolgáltatások nyújtására vonatkozó egyes törvényi, rendeleti vagy közigazgatási rendelkezéseinek összehangolásáról (Audiovizuális médiaszolgáltatásokról szóló irányelv).

²³ Az Európai Unió felülről lefelé történő szabályozása a tagállami védelmi szintek emelkedését is jelentette, szemben harmadik országok szabályozási szisztémáival. Ezt a hatást a szakirodalom szupranacionalizmus hatásnak vagy Brüsszel-effektusnak nevezi; lásd például Paul QUINN: Research under the GDPR – A Level Playing Field for Public and Private Sector Research? 17(4) *Life Sciences, Society and Policy* (2021), <https://doi.org/10.1186/s40504-021-00111-z>.

Schrems panaszt nyújtott be az ír felügyeleti hatósághoz, kérve ezen adattovábbítások megtiltását. Arra hivatkozott, hogy az Amerikai Egyesült Államok joga a továbbított személyes adatai tekintetében nem biztosítja a megfelelő védelmi szintet. A panasz elutasítására azért került sor, mert a Bizottság a 2000/520 határozatában²⁴ (biztonságos kikötő határozat²⁵) megállapította az Egyesült Államok megfelelő védelmi szintjét. Ugyanakkor a határozat megtámadása nyomán indult bírósági felülvizsgálatban az ír High Court érvénytelennek nyilvánította,²⁶ majd az előzetes döntéshozatali eljárást követően folytatódó alapeljárásban megsemmisítette a felügyeleti szerv határozatát.

Az ír felügyeleti hatóság ezt követő felhívására Schrems újrafogalmazott panaszában – az időközben megszületett 2010/87 határozattal²⁷ összefüggésben is – fenntartotta az elégséges védelem nyújtásának hiányára való hivatkozást. Kérte, hogy *ex nunc* hatállyal tiltsák el a jogsértő magatartást tanúsító Facebook Irelandet személyes adatainak az Európai Unióból az Egyesült Államokba továbbításától. A felügyeleti hatóság a panasz elbírálásának felfüggesztése mellett eljárást indított a High Courtnál annak érdekében, hogy az megítélhesse a 2010/87 határozat érvényességét. A High Court előzetes döntéshozatali eljárást kezdeményezett, majd a Bizottság elfogadta az EU–USA adatvédelmi pajzs által biztosított védelem megfelelőségéről szóló 2016/1250 határozatot²⁸ (adatvédelmi pajzs határozat).

Az EUB az Alapjogi Chartát szem előtt tartó vizsgálata alapján nem látta szükségesnek megállapítani a 2010/87 határozat érvénytelenségét,²⁹ miután az tartalmaz olyan hatékony mechanizmusokat, amelyek a gyakorlatban lehetővé teszik az uniós jog által megkövetelt védelmi szint biztosítását, továbbá azt is, hogy a kikötések megsértése esetén felfüggeszsek vagy megtiltsák a személyes adatok továbbítását.

Ugyanakkor más következtetésre jutott az EUB az adatvédelmi pajzs határozattal kapcsolatban: azt a GDPR szabályainak az Alapjogi Charta magán- és családi élet tiszteletben tartására, a személyes adatok védelmére és a hatékony bírói jogvédelemre vonatkozó rendelkezései fényében érvénytelennek nyilvánította.³⁰ Megállapította, hogy az adatvédelmi pajzs határozat – a korábban már általa érvénytelennek kimondott biztonságos kikötő határozathoz hasonlóan – a nemzetbiztonság, a közérdek és a bűnüldözés követelményeinek elsőbbségét fejezi ki, és

²⁴ A Bizottság határozata (2000. július 26.) a 95/46/EK európai parlamenti és tanácsi irányelv alapján, az Egyesült Államok Kereskedelmi Minisztériuma által kiadott biztonságos kikötő adatvédelmi elvek által biztosított védelem megfelelőségéről és az ezzel kapcsolatos gyakran felvetődő kérdésekről.

²⁵ Alessandro El KHOURY: The Safe Harbour is not a Legitimate Tool Anymore. What Lies in the Future of EU–USA Data Transfers? 6(4) *European Journal of Risk Regulation* (2015), <https://doi.org/10.1017/S1867299X00005237>, 659–664.

²⁶ C-362/14 Schrems.

²⁷ A Bizottság (EU) 2016/2297 végrehajtási határozata (2016. december 16.) a 95/46/EK európai parlamenti és tanácsi irányelv alapján a személyes adatok harmadik országokba és harmadik országbeli adatfeldolgozók részére történő továbbítására vonatkozó általános szerződési feltételekről szóló 2001/497/EK és 2010/87/EU határozatok módosításáról.

²⁸ A Bizottság (EU) 2016/1250 végrehajtási határozata (2016. július 12.) a 95/46/EK európai parlamenti és tanácsi irányelv alapján az EU–USA adatvédelmi pajzs által biztosított védelem megfelelőségéről.

²⁹ C-311/18 Facebook Ireland és Schrems.

³⁰ Marc ROTENBERG: Schrems II, from Snowden to China: Toward a New Alignment on Transatlantic Data Protection. 26(1–2) *European Law Journal* (2020) 141–152., <https://doi.org/10.1111/eulj.12370>.

lehetővé teszi a beavatkozást azon személyek alapvető jogaiba, akiknek az adatait az EU-ból harmadik országba továbbítják. Az EUB szerint a személyes adatok védelmének az Egyesült Államok belső szabályozásából eredő korlátozásai, különösen a továbbított adatokhoz való hozzáférés tekintetében, nem felelnek meg az uniós jogban az arányosság elvének érvényesülése érdekében meghatározott követelményeknek.³¹ Az Egyesült Államok belső szabályai a szükséges mértéket meghaladón is lehetővé teszik megfigyelési programok végrehajtását, amelyek esetében sem a felhatalmazás korlátozása, sem pedig az érintett nem amerikai személyek jogait védő garanciák, különösen a bíróságok előtt érvényesíthető jogosultságok nem biztosítottak. A bírói jogvédelem helyettesítésére az adatvédelmi pajzs határozatban szereplő ombudsmani mechanizmus nem alkalmas, mert az egyáltalán nem biztosít az érintett személyek számára megfelelő jogorvoslati lehetőséget. Az ombudsman ebben az összefüggésben nem rendelkezik az uniós jogban megkövetelt jogosultságokkal – nincsen az amerikai hírszerzési szervezetekkel szemben normatív szabályokkal rendezett, kötelező erejű határozatok hozatalára vonatkozó hatásköre, ami megfelelő jogvédelem nyújtását eredményezné –, ezáltal az ombudsman uniós jogban elvárt függetlensége sem biztosított.³²

Az ítélet tanulságaként megállapíthatjuk,³³ hogy az EUB alkalmazhatónak ítélte a GDPR-t a személyes adatoknak egy uniós tagállamban letelepedett gazdasági szereplő által valamely harmadik országban letelepedett másik gazdasági szereplőnek kereskedelmi célból végzett továbbítása szabályozására. Az EUB kimondta, hogy az adatkezelésre még akkor is irányadó a GDPR, ha az adatokat a továbbítás során vagy azt követően az érintett harmadik ország hatóságai közbiztonsági, honvédelmi és nemzetbiztonsági célból kezelhetik.³⁴ Az EUB úgy ítélte meg, hogy a megfelelő garanciákra, az érvényesíthető jogokra és a hatékony jogorvoslati lehetőségekre vonatkozó GDPR-szabályokat csak akként lehet értelmezni, hogy azoknak, akiknek a személyes adatait az általános adatvédelmi kikötések alapján továbbítják harmadik országba, olyan védelmi szinttel kell rendelkezniük, amely lényegében azonos az EU-ban biztosított védelmi szinttel. E védelmi szint értékelésénél figyelembe kell venni egyfelől az Alapjogi Charta rendelkezéseit, mert csak azok fényében lehetséges értelmezni az EU-ban letelepedett adatkezelő és a harmadik országban letelepedett címzett között létrejött szerződés GDPR-ben rögzített kikötéseit, másfelől – az így továbbított adatokhoz való esetleges hatósági hozzáférést illetően – a harmadik ország jogrendszerének releváns elemeit.

³¹ Marco DWORSCHAK: Auswirkungen von Schrems II auf den Steuerdatentransfer. *Liechtensteinische Juristen-Zeitung* (2020) 295–309.

³² Az EUB ítélkezési gyakorlata alapján egy szerv nem vonható a bírói jogvédelmet biztosítani hivatott bíróság autonóm uniós jogi fogalma alá, ha – egyéb feltételek mellett – nem felel meg a függetlenség kritériumának. A fogalmat az EUB az Európai Unió működéséről szóló szerződés 267. cikkének értelmében vett tagállami bíróság fogalmára vonatkozó ítélkezési gyakorlata során alakította ki, és olyan tényezők kimondásával írta körül, amelyeknek az adott fórumnak meg kell felelnie. E feltételek közé tartozik, hogy törvény alapján jött létre, állandó jelleggel működik, hatásköre kötelező jellegű, az eljárása kontradiktórium jellegű, jogszabályokat alkalmaz, független és pártatlan. A fogalom értelmezésével kapcsolatban lásd például GOMBOS Katalin: *Európai jog – az Európai Unió jogrendszere*. Budapest, Wolters Kluwer, 2019, <https://doi.org/10.55413/9789632959283>, 114–127.

³³ Xavier TRACOL: „Schrems II”: The Return of the Privacy Shield. 39 *Computer Law & Security Review* (2020), <https://doi.org/10.1016/j.clsr.2020.105484>.

³⁴ Ebből a megállapításból következik, hogy a GDPR hatálya alóli kizáráshoz ezek az adatkezelésre vonatkozó, az adatkezelés típusát meghatározó hivatkozások nem elégségesek.

A felügyeleti hatóságoknak tehát kötelezettségük felfüggeszteni vagy megtiltani a személyes adatok harmadik országba továbbítását, ha úgy vélik, hogy ott nem tartják be az általános adatvédelmi szabályokat, azokat ott nem lehet tiszteletben tartatni, vagy a továbbított adatok uniós jog által megkövetelt védelme más eszközzel nem biztosítható, mert az EU-ban letelepedett adatkezelő maga nem függesztette fel vagy fejezte be az ilyen továbbítást.

2.2. A felügyeleti hatóságok jogköreinek bővülése

A Facebook Ireland ügyben³⁵ az alapügy tényállása szerint a magánélet védelméért felelős belga bizottság (CBPL) elnöke keresetet nyújtott be a brüsszeli holland nyelvű elsőfokú bírósághoz a Facebook Ireland, a Facebook Inc. és a Facebook Belgium ellen az adatvédelemre vonatkozó jogszabályok feltételezett megsértése miatt. E jogsértések többek között a Facebook-fiókkal rendelkező és nem rendelkező belga internethasználók szörfözési szokásaira vonatkozó adatok (például a felkeresett oldal címe, az oldal látogatójának IP-címe vagy a megtekintés dátuma és időpontja; *cookies*), a beépülő közösségimédia-modulok (például „tetszik” vagy „megosztás” gomb; *social plug-ins*) gyűjtésében és felhasználásában álltak. Az első fokon eljáró tagállami bíróság megállapította, hogy a Facebook közösségi hálózat nem tájékoztatta kellőképpen a belga internethasználókat az adatok gyűjtéséről és felhasználásáról, emellett a bíróság érvénytelennek nyilvánította a felhasználóknak az említett adatok gyűjtéséhez és kezeléséhez adott mechanikus hozzájárulását.

A következő szakaszban a brüsszeli fellebbviteli bíróság kizárólag a Facebook Belgium által benyújtott kérelem vonatkozásában állapította meg az illetékességét. Kétségei merültek fel azzal kapcsolatban, hogy a GDPR-ban előírt egyablakos ügyintézési mechanizmus nem befolyásolja-e az adatvédelmi hatóság illetékességét, ezért előzetes döntéshozatali kérelemmel fordult az EUB-hez, az pedig pontosította a nemzeti felügyeleti hatóságoknak a GDPR alapján fennálló hatásköreit. A határokon átnyúló adatkezelések tekintetében a GDPR előírja az egyablakos ügyintézési mechanizmust,³⁶ amely a feladatoknak a fő felügyeleti hatóság és a többi érintett nemzeti felügyeleti hatóság közötti megosztásán alapul. Az EUB ítélezési gyakorlatából az következik, hogy minden egyes felügyeleti hatóság a saját tagállamának területén illetékes a GDPR alapján ráruházott feladatok végzésére és hatáskörök gyakorlására.³⁷ Ugyanakkor a mechanizmus szoros, lojális és hatékony együttműködést, bizonyos kérdésekben pedig a kölcsönös elismeréshez³⁸ hasonló elv alkalmazását követeli meg az adatvédelmi hatóságok között a személyes adatok védelmére vonatkozó szabályok következetes és egységes alkalmazásának biztosítása, ily módon e védelem hatékony érvényesülésének megőrzése érdekében.

³⁵ C-645/19 Facebook Ireland és társai.

³⁶ Lorna WOODS: Facebook Ireland and the One Stop Shop under the GDPR. *European Law Review* (2021) 685–691.

³⁷ C-311/18 Facebook Ireland és Schrems [147].

³⁸ Az EUB a C-120/78 Rewe kontra Bundesmonopolverwaltung für Branntwein ügyben hozott ítéletében kimondta, hogy a tagállamokban jogszerűen gyártott és forgalomba hozott bármely termékeket minden más tagállam piacán engedélyezni kell. Ez a kölcsönös elismerés elve, amelyet harmonizáció hiányában a tagállamok alkalmaznak egymás szabályaira vonatkozóan. Az elv a későbbiekben a jogharmonizáció egyik alapvető eszközeként érvényesült, és mára többek között az EU-n belüli igazságügyi együttműködés szervezőelvé is vált.

A rendelet értelmében főszabály szerint a fő felügyeleti hatóság jogosult azt megállapítani, hogy a határokon átnyúló adatkezelés szabálysértő [60. cikk (7) bekezdés] – a nemzeti felügyeleti hatóságok ilyen határozat elfogadására csak kivételes esetekben jogosultak [56. cikk (2) bekezdés és 66. cikk]. Az együttműködési mechanizmus lényege az, hogy a fő felügyeleti hatóság hatáskörének gyakorlása során nem hagyhatja figyelmen kívül a többi érintett felügyeleti hatóság álláspontját, és az azok egyike által emelt bármely releváns és megalapozott kifogás – legalábbis ideiglenesen – megakadályozza a fő felügyeleti hatóság döntéstervezetének elfogadását.

Az EUB szerint a hatékony jogorvoslathoz való jog biztosíthatósága érdekében a GDPR rendelkezéseit úgy kell értelmezni, hogy a határokon átnyúló adatkezelés vonatkozásában a nemzeti felügyeleti hatóságoknak is jogosultnak kell lenniük arra, hogy a rendelet bármely állítólagos megsértéséről tájékoztassák az igazságügyi hatóságokat és adott esetben bírósági eljárást kezdeményezzenek. Ennek feltétele egyrészt az, hogy a GDPR biztosítson hatáskört a nemzeti felügyeleti hatóságok számára az adatkezelés tekintetében fennálló jogsértést megállapító határozat elfogadására, másrészt e hatáskört a rendeletben előírt együttműködési és egységességi eljárások tiszteletben tartásával kell gyakorolni. A tagállami felügyeleti hatóság bírósági eljárás kezdeményezésére vonatkozó hatáskörének gyakorlása nem követeli meg [58. cikk (5) bekezdés], hogy a határokon átnyúló személyesadat-kezelés szempontjából adatkezelőnek vagy adatfeldolgozónak minősülő azon személy, aki ellen az eljárást kezdeményezik, e tagállam területén tevékenységi központtal vagy más tevékenységi hellyel rendelkezzen, de azt igen, hogy a jogsértés a GDPR területi hatálya alá tartozzon. Ebbe a kategóriába az EU-ban tevékenységi hellyel rendelkező adatkezelők vagy adatfeldolgozók attól függetlenül beletartoznak, hogy az adatkezelés az EU területén történik vagy sem [3. cikk (1) bekezdés].

Az EUB kimondta, hogy a tagállami felügyeleti hatóság a GDPR feltételezett megsértése miatt az adatkezelőnek mind az adott tagállamban, mind a másutt található tevékenységi helye tekintetében keresetet nyújthat be.³⁹ E jog gyakorlásának feltétele az, hogy a bírósági kereset az adott tevékenységi helyen végzett adatkezelésre vonatkozzon, a hatóság jogosult legyen e hatáskör gyakorlására, és a GDPR alkalmazható legyen az adott alapügyben.⁴⁰

Az EUB az ügyben rendezte a korábban hatályos adatvédelmi irányelv alapján megindult eljárásoknál a kereset fenntarthatóságának, továbbá a GDPR hatálybalépése után elkövetett jogsértések miatt indított eljárások kezdeményezésének a feltételeit is. Más szempontból is tisztázódott az ügyben releváns európai jogi kérdés, ugyanis az EUB elismerte a GDPR azon rendelkezésének közvetlen hatályát, amelynek értelmében a tagállamok jogszabályban előírják felügyeleti hatóságuk hatáskörrel rendelkezését arra, hogy e rendelet megsértéséről tájékoztassa az igazságügyi hatóságokat, és adott esetben bírósági eljárást kezdeményezzen.⁴¹ Következésképpen az ilyen hatóság akkor is hivatkozhat közvetlenül a GDPR-ra kereseti kérelmének meg-

³⁹ Thibault DOUVILLE: L'institutionnalisation du droit européen des données à caractère personnel. *Revue des affaires européennes*, 2021/2., 429–435.

⁴⁰ Az alapügyben a Facebook-csoport Belgiumban található tevékenységi helyének tevékenységei elválaszthatatlanul kapcsolódtak a releváns személyesadat-kezeléshez. Az EU területén a Facebook Ireland minősült adatkezelőnek, az adatkezelő tevékenységeivel összefüggésben végzett tevékenység ennélfogva a GDPR hatálya alá tartozott.

⁴¹ Pierrick BRUYAS: Droits fondamentaux – protection des données personnelles. *Europe*, 2021/8–9., Comm. 274.

alapozásához⁴² magánszemélyek elleni kereset indításakor vagy folytatásakor, ha azt kifejezetten nem hajtották végre az érintett tagállam jogszabályaiban.⁴³

2.3. Egy magyar eset tanulságai

A közelmúltban volt alkalma az EUB-nek egy magyar előzetes döntéshozatali előterjesztés alapján állást foglalni abban a kérdésben, hogy a felügyeleti hatóság az érintett előzetes kérelmének hiányában is jogosult-e elrendelni a jogellenesen kezelt adatok törlését.⁴⁴ Az ügy tényállása szerint Újpest Önkormányzata 2020 februárjában úgy határozott, hogy – egy egyébként nemes cél érdekében – a Covid-19-világjárvány veszélyeztetett csoportjába tartozó, meghatározott jogosultsági feltételeknek megfelelő lakosoknak anyagi támogatást biztosít. A magyar felügyeleti hatóság, amelyhez közérdekű bejelentés érkezett, megállapította, hogy Újpest Önkormányzata, a Magyar Államkincstár és a Kormányhivatal megsértette a GDPR rendelkezéseit, és jogkövetkezményként bírságokat szabott ki. A felügyeleti hatóság megállapította, hogy Újpest Önkormányzata az erre előírt egy hónapon belül nem nyújtott tájékoztatást az érintetteknek sem az adataik kezeléséről, sem annak céljáról, sem adatvédelmi jogaikról. A hatóság arra utasította Újpest Önkormányzatát, hogy törölje azoknak az érintetteknek a személyes adatait, akik jogosultak lettek volna a támogatást igénybe venni, de azt nem kérték. Újpest Önkormányzata a Fővárosi Törvényszék előtt támadta meg a határozatot, bírósági jogorvoslatot kérve. Álláspontja az volt, hogy a felügyeleti hatóság nem jogosult arra, hogy a személyes adatok törlését anélkül rendelje el, hogy az érintett e célból előzetesen kérelmet terjesztett volna elő. A közigazgatási határozatot felülbíráló testület az EUB-hez fordult előzetes döntéshozatali kérelemmel, amelyben a GDPR értelmezését kérte.

Az EUB a felügyeleti hatóság jogköreit vizsgálva megállapította, hogy a tagállami felügyeleti hatóság hivatalból – azaz még az érintett erre irányuló előzetes kérelme hiányában is – elrendelheti a jogellenesen kezelt adatok törlését, ha az szükséges a GDPR teljes körű tiszteletben tartásához. Ha ugyanis e hatóság azt állapítja meg, hogy egy adatkezelés nem felel meg a GDPR rendelkezéseinek, orvosolnia kell a megállapított jogsértést. Ebben az ügyben jogvédelmi célú, az adatvédelem sajátosságait és a versengő jogok összemérését is tiszteletben tartó jogértelmezés történt – az EUB szerint ha a felügyeleti hatóság csak az érintett kérelmére tartathatná be a GDPR rendelkezéseit, akkor az adatkezelő a kérelem hiányában megőrizhetné a szóban forgó személyes adatokat és azokat továbbra is jogellenesen kezelhetné. Természetesen ebből a jogértelmezésből *a maiore ad minus* következik, hogy a tagállami felügyeleti hatóság a jogellenesen kezelt személyes adatok törlését a közvetlenül az érintettől származó kérelem alapján is elrendel-

⁴² Sebastian BRETTHAUER: Extended Powers for Other Supervisory Authorities Concerned in the Case of Cross-Border Data Processing: Facebook Ireland. Case C-645/19 Facebook Ireland Ltd and Others v. Gegevensbeschermingsautoriteit. 59 *Common Market Law Review* (2022), <https://doi.org/10.54648/COLA2022101>, 1543–1556.

⁴³ Lásd még GOMBOS Katalin: A Digital Services Act és a Digital Markets Act várható kihívásai a jogalkalmazásban. *In Medias Res*, 2023/2., 92–119., <https://doi.org/10.59851/imr.12.2.5>.

⁴⁴ C-46/23 Újpesti Polgármesteri Hivatal.

heti, ez azonban a jogvédelmi feladatok elláthatóságára tekintettel előfeltételként nem követelhető meg.⁴⁵

2.4. Adatvédelem és versenyjog

A Meta Platforms-ügyben hozott ítélet⁴⁶ alapjául az „off-Facebook” adatok kezelése szolgált. A Meta Platforms Ireland kezeli a Facebook-hálózatot az EU-ban. Ha egy felhasználó regisztrál a Facebookra, ezzel elfogadja az e társaság által meghatározott általános szerződési feltételeket, amelyek – egyebek mellett – adatkezelési és *cookie*-szabályzatot is magukban foglalnak. E szabályzatok értelmében a Meta Platforms Ireland jogosult adatokat gyűjteni a felhasználók közösségi hálózaton belüli és azon kívüli tevékenységével kapcsolatban, és ezeket az adatokat összekapcsolni az érintett felhasználók Facebook-fiókjaival. Ezekből az ún. off-Facebook adatokból különösen harmadik felek weboldalainak és alkalmazásainak megtekintésére, valamint a Meta-csoporthoz tartozó egyéb online szolgáltatások (többek között az Instagram és a WhatsApp) használatára vonatkozó információk nyerhetők, amelyek révén lehetővé válik a Facebook-felhasználóknak szóló célzott reklámüzenetek készítése, a felhasználók profilozása vagy a reklámok személyre szabása.

A Meta Platforms-ítélet érdekessége, hogy először a német hatóság, majd az EUB verseny-szabályok vizsgálatán keresztül jutott adatvédelmi kérdésekben való állásfoglalásra.⁴⁷ A német szövetségi versenyhatóság megtiltotta a Meta-csoporthoz tartozó vállalkozásoknak, hogy a németországi felhasználók számára a Facebook használatát az off-Facebook adataik hozzájárulásuk nélküli kezelésétől tegyék függővé. Megállapította, hogy a szóban forgó adatok kezelése nem felelt meg a GDPR-nak, és a Meta visszaélt erőfölényével. Az EUB, amelyhez egy német bíróság fordult a Meta által e tilalommal szemben kezdeményezett jogvita keretében, kimondta, hogy egy tagállam versenyhatósága jogosult arra, hogy az erőfölénnyel való visszaélés vizsgálata keretében megállapítsa a GDPR megsértését, azonban a különös felügyeleti hatóságokkal együtt kell működnie. Ha a vizsgált magatartás már tárgyát képezte a felügyeleti hatóságok vagy az EUB határozatának, akkor a versenyhatóságot kötik a GDPR-ral kapcsolatos értékelések.

Az EUB döntött arról a kérdésről is, hogy a „különleges” adatok kezelése, ami a GDPR alapján főszabály szerint tiltott, kivételesen megengedhető-e olyan esetekben, amikor az érintett ezeket az adatokat kifejezetten nyilvánosságra hozta. Az EUB kimondta, hogy önmagában az a tény, hogy a felhasználó olyan weboldalakat vagy alkalmazásokat nyit meg, amelyek különleges adatokra utalhatnak, például faji vagy etnikai származásra, politikai véleményre, vallási meggyőződésre vagy szexuális irányultságra, nem jelenti azt, hogy adatait a GDPR értelmében kifejezetten nyilvánosságra hozza. Ugyanez vonatkozik arra az esetre is, ha a felhasználó adatokat visz be, vagy ha beépített kiválasztási gombokra kattint, kivéve, ha előzetesen kifejezetten kinyilvánította azt a döntését, hogy ezeket az adatokat korlátlan számú személy

⁴⁵ Pierrick BRUYAS: Données personnelles – effacement en cas de traitement illégal. *Europe*, 2024/5., Comm. 199.

⁴⁶ C-252/21 Meta Platforms és társai (Conditions générales d'utilisation d'un réseau social).

⁴⁷ Markus WÜNSCHELBAUM: Datenschutzrecht. Feststellung eines DS-GVO-Verstoßes durch nationale Wettbewerbsbehörde möglich. Anmerkung: EuGH (Große Kammer), Urteil vom 4.7.2023, C-252/21 (Meta Platforms Inc. ua/BKartA). *Europäische Zeitschrift für Wirtschaftsrecht* (2023).

számára nyilvánosan hozzáférhetővé teszi.⁴⁸ Az a tény, hogy a hálózat üzemeltetője erőfölényben van, nem zárja ki, hogy a felhasználó érvényesen és szabadon hozzájárulhasson adatainak kezeléséhez. Tekintettel azonban arra, hogy az ilyen erőfölényes helyzet érintheti a felhasználók választási szabadságát, fontos tényezőnek minősül annak meghatározása szempontjából, hogy a hozzájárulást érvényesen adták-e meg. A hozzájárulás meglétének bizonyítása az üzemeltető feladata.

A bemutatott esetek jól példázzák a hatósági feladatok⁴⁹ részbeni átrendeződését,⁵⁰ az új szemszögű,⁵¹ adatvédelmi rezilienciájú,⁵² a felhasználói érdekeket akár hivatalból is felismerő, azaz ebben az értelemben jogvédelmi célú jogalkalmazási attitűdjeinek megjelenését.⁵³

2.5. Irányelvi szabályok értelmezése

Az EUB C-178/22 számú ítéletében a magánélet védelme és a súlyos bűncselekmények üldözéséhez fűződő érdekek összemérésével hozott határozatot.⁵⁴ Ebben az ügyben a telefonszolgáltatás és az adatvédelem metszéspontjáról adott értelmezésében az EUB kimondta, hogy annak a bíróságnak, amelyet azzal bíztak meg, hogy engedélyezze a telefonhasználati adatokhoz való hozzáférést olyan bűncselekmények elkövetőinek azonosítása céljából, amelyek üldözéséhez a nemzeti jog ilyen hozzáférést ír elő, jogosultnak kell lennie arra, hogy megtagadja vagy korlátozza e hozzáférést. Az előzetes döntéshozatali kérelmet előterjesztő olasz bíróság tagállami joga szerint a minősített lopás azon bűncselekmények közé tartozik, amelyek igazolják a telefonhasználatra vonatkozó adatoknak az elektronikus hírközlési szolgáltatótól előzetes bírósági engedély alapján történő beszerzését. Az EUB megállapította, hogy az ilyen adatokhoz való hozzáférés csak a súlyos bűncselekményben való részvétellel gyanúsított személyek adatai tekintetében biztosítható, és pontosította, hogy a súlyos bűncselekmények fogalmát a tagállamoknak kell meghatározniuk. Az e hozzáférés engedélyezésével megbízott bíróságnak azon-

⁴⁸ Ana-Maria HRISCU: C-252/21 *Meta v Bundeskartellamt*: The Lawfulness of Big Tech's Processing of Personal Data and the Relationship Between Data Protection and Competition Law. 9(3) *European Data Protection Law Review* (2023), <https://doi.org/10.21552/edpl/2023/3/15>, 371–377.

⁴⁹ Inge GRAEF: *Meta Platforms: How the CJEU Leaves Competition and Data Protection Authorities with an Assignment*. 30(3) *Maastricht Journal of European and Comparative Law* (2023), <https://doi.org/10.1177/1023263X231205836>, 325–334.

⁵⁰ Peter G. PIGHT: CJEU on Facebook: GDPR Processing Justifications and Application Competence: EuGH, Urt. vom 4.7.2023, C-252/21 *Gewerblicher Rechtsschutz und Urheberrecht* (2023) 1169–1172.; Anno HABERER: The Neverending Story: Neues zum Verhältnis von Kartell- und Datenschutzrecht [EuGH, Urt. v. 4.7.2023, C-252/21 *Meta Platforms Inc. u.a./BKartA*]. *Neue Zeitschrift für Kartellrecht* (2023) 546–549.

⁵¹ Peter J. van de WAERDT: *Meta v Bundeskartellamt*: Something Old, Something New. 8(3) *European Papers* (2023) 1077–1103.

⁵² Francesco RIZZUTO: The Implications of the Meta Ireland Platforms Ruling for the Powers of National Competition Authorities and National Regulatory and Supervisory Authorities. 44(12) *European Competition Law Review* (2023) 532–538.

⁵³ Paolisa NEBBIA: The Interaction of Competition, Consumer and Data Protection Laws: A Few Comments Inspired by the Recent Case Law of the Court of Justice of the European Union. 23(4) *ERA-Forum: Scripta Iuris Europaei* (2023), <https://doi.org/10.1007/s12027-023-00733-0>, 515–527.

⁵⁴ C-178/22 *Procura della Repubblica presso il Tribunale di Bolzano*.

ban jogosultnak kell lennie arra, hogy megtagadja vagy korlátozza a hozzáférést, ha az a magánélet tisztelőben tartásához és a személyes adatok védelméhez való alapvető jogokba való súlyos beavatkozásnak minősül, még akkor is, ha a szóban forgó bűncselekményt az adott tagállamban – a fennálló társadalmi feltételekre tekintettel – nem tekintik súlyosnak.

Az alapügyben eljáró bolzanoi ügyészség egy minősített lopással kapcsolatos bűnügyi nyomozás keretében azt kérte az olasz bíróságtól, hogy az elkövetők azonosítása céljából engedélyezze az ellopott telefonkészülékek használatára vonatkozó adatok begyűjtését a telefontársaságoktól. Az EUB megállapította, hogy ez az alapvető jogokba való súlyos beavatkozásnak minősíthető, és megerősítette, hogy a telefonhasználati adatokhoz való hozzáférés csak a súlyos bűncselekményben való részvétellel gyanúsított személyek adatai tekintetében biztosítható. Kifejtette, hogy a GDPR alkalmazásához a súlyos bűncselekmények fogalmát a tagállamoknak kell meghatározniuk, ugyanis a büntetőjogi szabályozás tagállami hatáskörbe tartozik, ha az EU nem alkotott jogszabályt e jogterületen.

Ugyanakkor a tagállamok nem ferdíthetik el e fogalom jelentését, és ezt kiterjesztve a súlyos bűnözés fogalmát sem oly módon, hogy abba olyan bűncselekményeket is belevesznek, amelyek az adott tagállamban nyilvánvalóan nem súlyosak, még ha e tagállam jogalkotója elő is írta, hogy azok három évig terjedő szabadságvesztéssel büntetendők. Az EUB szerint az ilyen büntetésre való hivatkozással meghatározott küszöb nem tűnik túlzottan alacsonynak. Ezenfelül nem feltétlenül ellentétes az arányosság elvével, ha olyan küszöb kerül meghatározásra, amelytől kezdve a bűncselekményre kiszabható szabadságvesztés büntetési tétel felső határa megalapozza azt, hogy e bűncselekmény súlyosnak minősüljön. Azonban mindemellett lényeges – különösen annak ellenőrzéséhez, hogy a súlyos bűnözés fogalmát ne tágtásák ki túlzottan –, hogy ha a megőrzött adatokhoz való hozzáférés az érintett személy alapvető jogaiba való súlyos beavatkozás kockázatával jár, akkor a hozzáférés bíróság vagy független közigazgatási szerv által végzett előzetes felülvizsgálat tárgyát képezze. Az előzetes felülvizsgálatot végző bíróságnak képesnek kell lennie arra, hogy megfelelő egyensúlyt teremtsen a nyomozás szükségletei és a magánélet tisztelőben tartásához, a személyes adatok védelméhez fűződő alapvető jogok között.

Az EUB a C-470/21 ítéletben a bűncselekmények elleni küzdelem és az alapvető jogokba való beavatkozás ütköző helyzetét vizsgálta.⁵⁵ Megállapította, hogy az online elkövetett hamisítások elleni küzdelemért felelős nemzeti hatóság hozzáférhet az IP-címhez rendelt azonosító adatokhoz. Az EUB pontosította az ezen adatok megőrzése és az azokhoz való hozzáférés követelményeit: a tagállamok előírhatják az internet-hozzáférést nyújtó szolgáltatóknak az IP-címek általános és különbségtétel nélküli megőrzését általánosságban a bűncselekmények elleni küzdelem céljából, ha a megőrzés nem teszi lehetővé az érintett személy magánéletére vonatkozó pontos következtetések levonását. Ez olyan megőrzési módok révén valósítható meg, amelyek biztosítják az IP-címek és a személyes adatok egyéb kategóriái, különösen a személyazonosságra vonatkozó adatok valóban teljes elkülönítését. A tagállamok bizonyos feltételek mellett engedélyezhetik továbbá az illetékes nemzeti hatóság számára, hogy az IP-címeknek megfelelő, személyazonosságra vonatkozó adatokhoz hozzáférjen, feltéve, hogy biztosított a megőrzött adatok különböző kategóriáinak valóban teljes elkülönítése. Ha – atipikus helyzetekben – az

⁵⁵ C-470/21 La Quadrature du Net és társai.

ilyen hozzáférést szabályozó nemzeti eljárás sajátosságai a gyűjtött adatok és információk összekapcsolása révén lehetővé tehetik az érintett magánéletére vonatkozó pontos következtetések levonását, bíróságnak vagy független közigazgatási szervnek előzetesen felül kell vizsgálnia a hozzáférés engedélyezését.

A szerzői vagy szomszédos jogok hatálya alá tartozó műveknek az interneten elkövetett bűncselekményekkel szembeni védelme érdekében hozott rendelet két személyesadat-kezelést vezetett be. Az első abban áll, hogy a szerzőket képviselő szervezetek olyan IP-címeket gyűjtenek, amelyeket a *peer-to-peer* hálózatokon valószínűsíthetően ilyen bűncselekmények elkövetéséhez használtak, és e címeket a művek internetes terjesztésével és a jogok védelmével foglalkozó főhatóság (Hadopi) rendelkezésére bocsátják. A másodiknál az internet-hozzáférést nyújtó szolgáltató a Hadopi kérésére összekapcsolja az IP-címet és a jogosultjának személyazonosságára vonatkozó adatokat. Ezek az adatkezelések lehetővé teszik e hatóság számára, hogy az azonosított jogosultakkal szemben nevelési és megtorló intézkedéseket magában foglaló eljárást indítson, és azt a legsúlyosabb esetekben akár az ügyészség elé terjessze. A jogok és a szabadságok interneten való védelmével foglalkozó négy egyesület kérte a francia államtanácstól a szóban forgó rendelet megsemmisítését. Az államtanács azt kérdezte az EUB-től, hogy ezek az adatkezelések összeegyeztethetők-e az uniós joggal.

A teljes ülésben eljáró EUB úgy ítélte meg, hogy az IP-címek általános és különbségtétel nélküli megőrzése nem feltétlenül minősül az alapvető jogokba való súlyos beavatkozásnak, de csak akkor megengedett, ha a nemzeti szabályozás olyan megőrzési módokat ír elő, amelyek biztosítják a személyes adatok különböző kategóriáinak valóban teljes elkülönítését, és ily módon kizárják az érintett magánéletére vonatkozó pontos következtetések levonását. Az EUB rögzítette továbbá, hogy nem ellentétes az uniós joggal az olyan nemzeti szabályozás, amely lehetővé teszi az illetékes hatóság számára, hogy az internet-hozzáférést nyújtó szolgáltatók által valóban teljesen elkülönített módon megőrzött, az IP-címnek megfelelő, személyazonosságra vonatkozó adatokhoz kizárólag annak érdekében férjen hozzá, hogy azonosítani tudja a bűncselekmény elkövetésével gyanúsítható személyt. A tagállamoknak viszont biztosítaniuk kell, hogy e hozzáférés ne tegye lehetővé az IP-címek jogosultjainak magánéletére vonatkozó pontos következtetések levonását. Ez azt jelenti, hogy a hozzáféréssel rendelkező tisztviselők számára meg kell tiltani, hogy az általuk megtekintett fájlok tartalmára vonatkozó információkat bármilyen formában nyilvánosságra hozzák, a böngészési útvonalat az IP-címek alapján nyomon kövessék, és e címeket a jogosultjaiknak a velük szembeni esetleges intézkedésektől eltérő célra használják fel.

Ha az elektronikus hírközlési eszközök felhasználóinak személyazonosságára vonatkozó adatokhoz való hozzáférés kizárólagos célja az érintett felhasználó azonosítása, a hozzáférés bíróság vagy független közigazgatási szerv általi előzetes felülvizsgálata nem kötelező, feltéve hogy e hozzáférés nem jelent az alapvető jogokba való súlyos beavatkozást. E felülvizsgálatot azonban elő kell írni, ha az ilyen hozzáférést szabályozó nemzeti eljárás sajátosságai lehetővé tehetik az eljárás különböző szakaszaiban folyamatosan gyűjtött adatok és információk összekapcsolása révén az érintett személy magánéletére vonatkozó pontos következtetések levonását. Ilyen esetben a bíróság vagy független közigazgatási szerv általi felülvizsgálatot ezen összekapcsolás előtt kell elvégezni, megőrizve az eljárás hatékonyságát, lehetővé téve különösen a szóban forgó jogsértő magatartás esetleges megisméltéseinek felderítését.

3. Összegzés: az értelmezési elsődlegesség

A bevezetőben jelzett jogértelmezési sajátosságok és a bemutatott példák alapján következtethetünk arra, hogy mind a hatósági felügyeleti, mind a bírósági jogalkalmazás során szükség lehet jogvédelmi célú jogértelmezésre, amelynek dogmatikai alapját az értelmezési elsődlegesség elve képezheti.⁵⁶ Ez jelentéstartalma szerint – különösen irányelvi szabályok vagy hézagos tartalmú, nyitott tényállású, vagy a tagállami jogokra is visszautaló, a tagállami jogalkotásnak is helyet hagyó rendeleti keretszabályok esetén – egyrészt azt foglalja magában, hogy a tagállami jogalkalmazónak az előtte folyó ügyben úgy kell értelmeznie egy kizárólag a belső helyzetre kidolgozott nemzeti jogszabályt, hogy az alkalmazható legyen a határokon átnyúló adott tényállásra, másrészt autonóm uniós értelmezés szerinti tartalmat kell annak tulajdonítani. Ennek korlátja, hogy az értelmezés nem lehet jogszabályi előfeltételt pótló, azaz az értelmezési elsődlegesség nem szolgálhat magának az alanyi jognak a megteremtésére.

Az értelmezési elsődlegesség szoros összefüggésben áll a közvetett hatály (értelmezési doktrína) azon elvével is, amely szerint a tagállami bíróság köteles a tagállami jogot az uniós norma céljai és megfogalmazása szerint értelmezni. Az uniós jog céljával összhangban álló értelmezés kötelezettsége a tagállami jog rendelkezéseinek összességére vonatkozik, korlátait pedig csak az általános jogelvek alkotják, különösen a jogbiztonság elve, abban az értelemben, hogy e kötelezettség nem szolgálhat alapjául a tagállami jog *contra legem* értelmezésének.⁵⁷ A hatékony jogvédelem érdekében a felügyeleti hatóságoknak és az ilyen ügyekben eljáró bíróságoknak le kell folytatniuk a vizsgálatot – akár hivatalból felismerve a személyes adatok védelméhez fűződő nyomós érdekeket –, ezzel biztosítva az online szolgáltatások és az adatvédelmi jog találkozási pontjain a versengő jogok összemérésével, szükség szerint a szükségesség-arányosság teszt elvégzésével az értelmezési elsődlegesség sajátos megvalósítását.

Irodalomjegyzék

- ANDENAS, Mads – FAIRGRIEVE, Duncan: *Courts and Comparative Law*. Oxford, Oxford University Press, 2015, 117–232.
<https://doi.org/10.1093/acprof:oso/9780198735335.001.0001>
- BARNARD, Catherine: *The Substantive Law of the EU: The Four Freedoms*. Oxford, Oxford University Press, 2022.
<https://doi.org/10.1093/he/9780192857880.001.0001>
- BRETTAUER, Sebastian: Extended Powers for Other Supervisory Authorities Concerned in the Case of Cross-Border Data Processing: Facebook Ireland. Case C-645/19 Facebook Ireland Ltd and Others v. Gegevensbeschermingsautoriteit. 59 *Common Market Law Review* (2022) 1543–1556.
<https://doi.org/10.54648/COLA2022101>

⁵⁶ Lásd részletesebben GOMBOS Katalin: A jogértelmezés jelentősége a közösségi jogban – avagy az értelmezési elsődlegesség elvéről. *Európai Jog*, 2010/2., 3–10.

⁵⁷ C-605/21 Heureka Group (Compareurs de prix en ligne) [93].

- BRUYAS, Pierrick: Droits fondamentaux – protection des données personnelles. *Europe*, 2021/8–9., Comm. 274.
- BRUYAS, Pierrick: Données personnelles – effacement en cas de traitement illégal. *Europe*, 2024/5., Comm. 199.
- DOUVILLE, Thibault: L'institutionnalisation du droit européen des données à caractère personnel. *Revue des affaires européennes*, 2021/2., 429–435.
- DWORSCHAK, Marco: Auswirkungen von Schrems II auf den Steuerdatentransfer. *Liechtensteinische Juristen-Zeitung* (2020) 295–309.
- GOMBOS Katalin: A jogértelmezés jelentősége a közösségi jogban – avagy az értelmezési elsődlegesség elvéről. *Európai Jog*, 2010/2., 3–10.
- GOMBOS Katalin: *Európai jog – az Európai Unió jogrendszere*. Budapest, Wolters Kluwer, 2019.
<https://doi.org/10.55413/9789632959283>
- GOMBOS Katalin: A Digital Services Act és a Digital Markets Act várható kihívásai a jogalkalmazásban. *In Medias Res*, 2023/2., 92–119.
<https://doi.org/10.59851/imr.12.2.5>
- GRAEF, Inge: Meta Platforms: How the CJEU Leaves Competition and Data Protection Authorities with an Assignment. 30(3) *Maastricht Journal of European and Comparative Law* (2023) 325–334.
<https://doi.org/10.1177/1023263X231205836>
- HABERER, Anno: The Neverending Story: Neues zum Verhältnis von Kartell- und Datenschutzrecht [EuGH, Urt. v. 4.7.2023, C-252/21 Meta Platforms Inc. u.a./BKartA]. *Neue Zeitschrift für Kartellrecht* (2023) 546–549.
- HRISCU, Ana-Maria: C-252/21 Meta v Bundeskartellamt: The Lawfulness of Big Tech's Processing of Personal Data and the Relationship Between Data Protection and Competition Law. 9(3) *European Data Protection Law Review* (2023) 371–377.
<https://doi.org/10.21552/edpl/2023/3/15>
- KHOURY, Alessandro El: The Safe Harbour is not a Legitimate Tool Anymore. What Lies in the Future of EU-USA Data Transfers? 6(4) *European Journal of Risk Regulation* (2015) 659–664.
<https://doi.org/10.1017/S1867299X00005237>
- LENAERTS, Koen – GUTIÉRREZ-FONS, José Antonio: *Les méthodes d'interprétation de la Cour de justice de l'Union européenne*. Brussels, Bruylant, 2020.
- LENAERTS, Koen – GUTIÉRREZ-FONS, José Antonio: *Az Európai Unió Bíróságának jogértelmezési módszerei* (ford. LUKÁCS Adrienn, ORBÁN Endre, SIMON Emese Réka). Budapest, HVG-ORAC, 2022.
- NEBBIA, Paolisa: The Interaction of Competition, Consumer and Data Protection Laws: A Few Comments Inspired by the Recent Case Law of the Court of Justice of the European Union. 23(4) *ERA-Forum: Scripta Iuris Europaei* (2023) 515–527.
<https://doi.org/10.1007/s12027-023-00733-0>
- PICHT, Peter G.: CJEU on Facebook: GDPR Processing Justifications and Application Competence: EuGH, Urt. vom 4.7.2023, C-252/21 *Gewerblicher Rechtsschutz und Urheberrecht* (2023) 1169–1172.

- QUINN, Paul: Research under the GDPR – A Level Playing Field for Public and Private Sector Research? 17(4) *Life Sciences, Society and Policy* (2021).
<https://doi.org/10.1186/s40504-021-00111-z>
- RIZZUTO, Francesco: The Implications of the Meta Ireland Platforms Ruling for the Powers of National Competition Authorities and National Regulatory and Supervisory Authorities. 44(12) *European Competition Law Review* (2023) 532–538.
- ROTENBERG, Marc: Schrems II, from Snowden to China: Toward a New Alignment on Transatlantic Data Protection. 26(1–2) *European Law Journal* (2020) 141–152.
<https://doi.org/10.1111/eulj.12370>
- TRACOL, Xavier: „Schrems II”: The Return of the Privacy Shield. 39 *Computer Law & Security Review* (2020).
<https://doi.org/10.1016/j.clsr.2020.105484>
- VÁRADI Szilvia: Az információs társadalom iránti bizalom erősítését célzó szabályozási mód-szerek az uniós adatvédelem területén. In STRIHÓ Krisztina – SZEGEDI László (szerk.): *Európai szabályozáspolitikai kihívások*. Budapest, Ludovika, 2022, 195–204.
- VÖRÖS Imre: Európai jog – magyar jog: konkurencia vagy koezisztencia? *Jogtudományi Közlöny*, 2011/7–8, 369–401.
- WAERDT, Peter J. van de: Meta v Bundeskartellamt: Something Old, Something New. 8(3) *European Papers* (2023) 1077–1103.
- WOODS, Lorna: Facebook Ireland and the One Stop Shop under the GDPR. *European Law Review* (2021) 685–691.
- WÜNSCHELBAUM, Markus: Datenschutzrecht. Feststellung eines DS-GVO-Verstoßes durch nationale Wettbewerbsbehörde möglich. Anmerkung: EuGH (Große Kammer), Urteil vom 4.7.2023, C-252/21 (Meta Platforms Inc. ua/BKartA). *Europäische Zeitschrift für Wirtschaftsrecht* (2023).



SzakcikkAdatbázis

OLVASSA AZ ÖSSZES JOGI FOLYÓIRATOT A SZÁMÍTÓGÉPÉN!

Harmincnégy jogi szaklap 2000-től megjelent évfolyamai kutathatók a weboldalon.

SZAKCIKKADATBAZIS.HU

