arsboni

XIV. évfolyam 2026/1. szám

arsboni jogi folyóirat · arsboni.hu

Kiadja a Stádium Intézet
Budapest, Akadémia utca 11. mfsz. 3/A
stadiumintezet@gmail.com
arsboni@arsboni.hu
ISSN 2064-4655

TARTALOMJEGYZÉK

TANULMÁNY

Édes Krisztián:[1]

Visszalépés vagy evolúció? – Az európai elfogatóparancs és a kiadatás jogintézményének viszonya

Az európai elfogatóparancs 2004. január 1-je óta felváltotta a korábban működő hosszadalmas kiadatási eljárásokat. Elfogadásával egy hatékony és egyszerű átadási eljárás lépett hatályba, amely képes reagálni a minőségében megváltozott bűnözésre. Napjainkban azonban a tagállamok és az Európai Unió Bírósága is folyamatos kihívások elé állítja az európai elfogatóparancs jogintézményét és egyes aspektusaiban vissza-vissza nyúl a régi kiadatáshoz. Ennek tükrében célszerű feltérképezni az átadás és a kiadatás hatályos viszonyát és ismertetni az európai elfogatóparancs gyakorlatát. Tanulmányomban leíró és kritikai módszerrel elemzem a két jogintézmény viszonyát melyek következtében megállapítom, hogy szükséges az európai elfogatóparancs jelenlegi kereteinek újragondolása, hiszen annak fennmaradásához elengedhetetlen az alapjogvédelem és a hatékonyság közötti összhang megteremtése. A tanulmány rávilágít arra, hogy ha ezen tovább fejlesztés nem történik meg, akkor az európai elfogatóparancson kívül a kölcsönös bizalmon alapuló kölcsönös elismerés elve is veszélybe kerül.

I. Bevezetés

A szubjektív büntetőjog (*ius puniendi)* keretében az államnak joga van saját törvényei alapján, a joghatóság és az emberi jogokra vonatkozó nemzetközi korlátok betartása mellett a bűncselekményeket büntetni.[2] Nemzeti jogi szempontból a ius puniendi magába foglalja az értékválasztás, az eszközválasztás, a bűncselekmény és büntetések meghatározásának, a szigor alkalmazásának és a büntetés végrehajtásának hatalmát, valamint a büntetőjogi felelősség megállapításának jogát. Ezen részelemek érvényesítése a nemzetek alapvető érdekét képezik, hiszen bármely büntetőjogi rendszer legitimációja azon a feltételezésen alapul, hogy az állam rendelkezik a *ius puniendi* hatalmával.[3]

A XX. századi európai integráció ugyanakkor magával hozta az uniós polgárok szabad mozgását, ami leegyszerűsítette a bűnelkövetők határon átnyúló tevékenységét. Következésképpen az állami büntetőhatalom érvényesítése, valamint a későbbiekben egy, a szabadságon, biztonságon és a jog érvényesülésén alapuló térség kialakítása érdekében szükségessé vált egy szorosabb bűnügyi együttműködési rendszer létrehozása. Ezen

[1] Hallgató, Eötvös Loránd Tudományegyetem Állam- és Jogtudományi Kar.

[2] Aaron X. Fellmeth – Maurice Horwitz: *Guide to Latin in International Law.* Oxford University Press, New York, 2011, 183. o.

[3] Karsai Krisztina: Ius Puniendi of the European Union. In: Hack Péter – Koósné Mohácsi Barbara (szerk.): *Emberek őrzője: Tanulmányok Lőrincz József tiszteletére, 1. kötet.* ELTE Eötvös Kiadó, Budapest, 2014, 117-118. o.

kitétel megvalósulásának kiindulópontját a kiadatási eljárás jelentette, ami a kölcsönös elismerés elvén alapuló európai elfogatóparancs jogintézményének megalkotásában teljesedett ki.[4]

Tanulmányom kidolgozásához azon feltevéssel láttam hozzá, hogy az európai elfogatóparancs egy integrált Európának megfelelő eljárást hozott létre, melynek lefolyása gyors és egyszerű, illetve ami maga mögött hagyta a kiadatási eljárás jellemzőit. Ennek okán kéziratom célja áttekinteni az európai igazságügyi együttműködés egyik sarokkövét jelentő jogintézmény fejlődésének történetét, valamint ismertetni eljárását és összevetni azt az elődjének nevezhető európai kiadatási eljárással. Munkámban továbbá az európai elfogatóparancs eredményei mellett rávilágítok jelenlegi kihívásaira.

Dolgozatom szakmai relevanciájának indoka az európai elfogatóparanccsal kapcsolatos hatályos gyakorlat, mivel az Európai Unió Bírósága (a továbbiakban: EUB/Bíróság) napjainkban jogfejlesztési gyakorlatán keresztül háttérbe szorítja az európai elfogatóparancs hatékonyságát a terhelt alapvető jogainak védelme érdekében. E tekintetben egyre inkább visszanyúl a kiadatási eljárás eszméihez. Következésképpen érdemes vizsgálat tárgyává tenni a két intézmény közötti különbségeket, hiszen ily módon választ kapunk arra a kérdésre, hogy valóban érdemes-e visszatérni a kiadatás jogintézményéhez, annak egyes elveihez.

I.1. Alkalmazott módszertan

Tanulmányom során egyaránt alkalmaztam komparatív és kvalitatív elemzési módszereket. Elsőként a két jogintézmény kialakulását ismertetem és rávilágítok az európai elfogatóparancs megalkotásának szükségességére. Ezt követi a tanulmány összehasonlító része, ahol bemutatom a kiadatás és az átadás közti jelentős különbségeket, majd ismertetem az európai elfogatóparancs eredményeit. Tanulmányom utolsó fejezetében kritikai elemzés lefolytatását követően levonom következtetéseim az európai elfogatóparancs hatályos gyakorlatáról.

II. Történeti előzmények

A kiadatás jogintézményének alapjai az ókori birodalmak békeszerződéseire vezethetők vissza, melyekben a két fél megállapodott a fogvatartott alattvalóik kiadatásáról. Ehhez hasonló egyezmények folyamatos fejlődése vezetett az *„aut dedere aut judicare”* elv kialakulásához, amely a nemzetközi büntetőjogi együttműködés alapját képezi. Ezen elv minden bizonnyal már a XIV. században is jelen volt, bár megnevezésére csupán 1625-ben került sor Hugó Grotius *Háború és Béke* című könyvében, mint *„aut dedere, aut punire*”. A kifejezés általában „kiadni vagy büntetni” fordításban volt megtalálható,

[4] Ismertetők az Európai Unióról: *Büntetőügyekben folytatott igazságügyi együttműködés, Célkitűzések.* https://www.europarl.europa.eu/factsheets/hu/sheet/155/buntetougyekben-folytatott-igazsagugyi-egyuttmukodes (Letöltve: 2025. 12. 12.).

ennek oka, hogy ekkoriban vélhetően nem ismerték az „*extradere*” (kiadatás) igét, tartalmukat tekintve viszont összeegyeztethetők.[5]

Fontos megemlíteni, hogy az *aut dedere aut punire* jogot és nem pedig kötelezettséget jelentett. A megkeresett állam diszkrecionális mérlegelésre alapítva döntött a kiadatásról vagy a büntetőjogi felelősségre vonásról. Grotius álláspontja szerint a szuveréneknek nemzetközi kötelessége az elv betartása, a modern kiadatási jogban ezen kitétel nem feltétlenül érvényesül. Kérdéses az is, hogy az elv a nemzetközi szokásjog részének, általános elvnek vagy pedig egy nemzetközi szerződések elemének minősül-e?[6]

A világ más részeihez hasonlóan a kiadatás európai viszonylatban is - a mélyebb együttműködést megelőzően – multilaterális és bilaterális egyezmények útján történt, ezen szerződések alakították ki a kiadatási jog legjelentősebb alapelveit, például a viszonosság, a kettős büntethetőség és a specialitás elvét.[7] A viszonosság a nemzetközi jog egyik alapkövének tekintendő, melynek értelmében a jogsértő tudomással van arról, hogy ha nem tartja be az adott jogi normát vagy nemzetközi szerződést, ugyanolyan jogi hátrány érheti. A kettős büntethetőség értelmében csak akkor van lehetőség jogsegélynyújtásra, ha az értintett cselekmény a megkeresett állam joga szerint is bűncselekménynek minősül, míg a specialitás elve szerint kiadni kért személlyel szemben a kiadatása előtt elkövetett, de a kiadatás alapjául nem szolgáló egyéb bűncselekmény miatt a megkereső államban nem indítható büntetőeljárás, nem alkalmazható személyi szabadságot korlátozó kényszerintézkedés, és nem hajtható végre jogerősen kiszabott büntetés. Emellett a terheltet harmadik államnak sem adhatják ki vagy át. Ezen elvek nem csupán az államközi egyezményekben érvényesülnek, hanem részét képzik a hatályos európai elfogatóparancs szabályrendszerének.[8]

A második világháborút követően a további konfliktusok megelőzésének, valamint az „európai föderáció” alapjainak lefektetése céljából 1951-ben megkötötték az *Európai Szén- és Acélközösségről szóló szerződést* majd 1957-ben az Európai Gazdasági Közösséget és az Európai Atomenergia-közösséget létrehozó szerződéseket.[9] Utóbbi két szerződéssel egy időben 1957. december 13. napján Párizsban elfogadták az európai elfogatóparancsot megelőző legfontosabb dokumentumot: az *Európai Kiadatási Egyezményt* (továbbiakban: Kiadatási Egyezmény). Hazánkban a kommunista rendszer bukását követően az *1994. évi XVIII. a Párizsban, 1957. december 13-án kelt, európai kiadatási egyezmény és kiegészítő jegyzőkönyveinek kihirdetéséről szóló törvény* hirdette ki.

---

[5] M. Nyitrai Péter: A kiadatás intézménye a nemzetközi büntetőjogban – egy új korszak régi-új kihívásai Európában. *Publicationes Universitatis Miskolciensis / Sectio Juridica et Politica*, 2003, 103. o.

[6] M. Nyitrai Péter: A kiadatási jog nemzetközi forrásainak szerepe a terhelt jogvédelmének nézőpontjából. *Publicationes Universitatis Miskolciensis / Sectio Juridica et Politica*, 2001. 17. o.

[7] Polt Péter: A kiadatás alkonya – egy új jogintézmény az európai letartóztatási parancs. *Európai Jog: Az Európai Jogakadémia Folyóirata*, 2002/2., 3-8. o. https://szakcikkadatbazis.hu/doc/7062223 (Letöltve: 2025.12.12.).

[8] M. Nyitrai 2003: i.m. 103. o.

[9] Ismertetők az Európai Unióról: *Az első szerződések:* https://www.europarl.europa.eu/factsheets/hu/sheet/1/az-elso-szerzodesek (Letöltve: 2025. 12. 12.).

Az általános kiadatás mellett regionális szinten is kialakultak egyszerűsített kiadatási egyezmények. Ezek célja alapjaiban megegyezik a későbbi európai elfogatóparancséval, ugyanakkor továbbra is hordoznak a kiadatásra jellemző jegyeket, mint például a végrehajtás szélesebb körű megtagadása.

II.1. A kiadatási eljárás[10]

Mielőtt ismertetném az európai elfogatóparancs bevezetésének okát és az európai integrációra gyakorolt hatását, szükséges felvázolnom a kiadatási eljárás hazai menetét és annak európai viszonylatban való „kiöregedését".

A kiadatási eljárást kiadatási kérelem indítja, melyet főszabály szerint a megkeresett állam kompetens hatóságához – általában igazságügyi miniszterhez – írásban és diplomáciai úton kell előterjeszteni. A kérelem befogadását követően az igazságügyi miniszter – abban az esetben, ha a kiadatás nem sérti Magyarország közrendjét és alapvető nemzetbiztonsági érdekét – haladéktalanul megküldi a Fővárosi Törvényszéknek, aki dönt kiadatás feltételeinek fennállásáról, melyről a *nemzetközi bűnügyi jogsegélyről szóló 1996. évi XXXVIII. törvény 11-16. §* rendelkezik. A Fővárosi Törvényszék nem ügydöntő végzése ellen, amennyiben azt törvény nem zárja ki, fellebbezésnek van helye a Fővárosi Ítélőtáblához. Ha a törvényben meghatározott feltételek nem teljesülnek a bíróság döntésére való hivatkozással az igazságügyi miniszter köteles megtagadni a kiadatás teljesítését. A bíróság ellenkező döntése alapján az igazságügyi miniszter jogosult dönteni a kérelem megtagadásáról vagy teljesítéséről. [11]

Fontos továbbá ismertetni a kiadatási megkeresés tartalmi elemeit, melyek alapvetően különböznek az európai elfogatóparancs formanyomtatványában meghatározottaktól. A megkeresésnek tartalmaznia kell a nemzeti elfogatóparancsot, a bűnösséget megállapító, a büntetést kiszabó vagy biztonsági intézkedést elrendelő határozatot, a kiadni kért terhelt személyes adatait, a megkereső igazságügyi hatóság megnevezését, a megkereső állam kötelezettségvállalását a halálbüntetés, a specialitás elvének terén valamint az átadandó tárgyak meghatározott időn belül történő visszajuttatását illetően.[12] A kiadatási megkeresés mindezeken felül tartalmazza a kérelem tárgyát képző bűncselekmény tényállását, ami alapjául szolgál az imént ismertetett döntési eljárás lefolytatásának.

Ettől eltérően az egyszerűsített kiadatási eljárás során - a kérelemhez csatolt iratok alapján - a bíróság dönt, hogy a kiadatás nem ütközik-e nyilvánvalóan valamilyen feltételbe vagy, hogy fennállnak-e annak feltételei. Ha a terhelt hozzájárul, a kiadatás esetében nem érvényesül a specialitás elve. Az általános rendszertől további eltérés, hogy a kompetens hatóság előzetesen dönthet a kiadatás engedélyezéséről, ezzel tovább gyorsítva az eljárást.[13]

[10] A kiadatási eljárás bemutatása a magyar jogrend szabályain keresztül történik.
[11] A nemzetközi bűnügyi jogsegélyről szóló 1996. évi XXXVIII. törvény.
[12] M. Nyitrai 2003: i.m. 177-178. o.
[13] Uo. 183. o.

II.2. Az európai elfogatóparancs kialakulása

A *Schengeni Megállapodás és Egyezmény* 1985. június 14. napján történő aláírásával valamint az 1993. november 1. napján hatályba lépő *Európai Unióról szóló Szerződés* (továbbiakban: EUSZ) minden korábbinál szorosabb európai együttműködés valósult meg. Az Európai Unió létrejötte, a négy alapszabadság megvalósulása és a tagállami határok fellazulása magával hozta a bűncselekmények „európaizálódását". A fentebb ismertetett kiadatási eljárások ezen új környezetben nem minősültek megfelelő eszköznek tekintve, hogy a hosszadalmas eljárás gátat szabott a hatékony igazságszolgáltatásnak. Ily módon szükségessé vált egy új jogintézmény kidolgozása, mely megfelelően képes kezelni a minőségében megváltozott bűnözés hatásait és érvényre tudja juttatni az Európai Unió által lefektetett alapelveket.

A EUSZ *büntetőügyekben folytatott rendőrségi és igazságügyi együttműködésről* szóló VI. címe a tagállamok közös fellépésének kidolgozásával, ezen belül is a rendőrség és az igazságügyi szervek mélyreható együttműködésének megvalósításával kívánta elérni a térség magas szintű biztonságát.[14]

Ezen cím alatt megfogalmazott célok és elvek megvalósításának céljából az Európai Tanács (a továbbiakban: Tanács) 1999-ben Finnországban a tamperei csúcsértekezleten határozta meg azokat a pontokat, melyek mentén 2001. decemberében megalkották az európai elfogatóparancs jogintézményének javaslatát. A Tanács fő célként tűzte ki a kiadatási eljárás formalitásainak eltörlését a már jogerősen elítélt terhelteknél, az ilyen személyek kiadatása helyetti átadását, a kiadatási eljárás felgyorsítását, valamint a bírósági határozatok kölcsönös elismerésen alapuló elfogadását. Mindezek alapján 2002. június 13. napján létrejött a *2002/584/IB számú Az európai elfogatóparancsról és a tagállamok közötti átadási eljárásokról szóló kerethatározat* (továbbiakban: Kerethatározat).[15]

II.3. A kölcsönös elismerés elve

Az európai közösségi jogban régóta jelen van a kölcsönös elismerés elve. Magánjogi szempontból az áruk szabad mozgását biztosítja, mely abban az esetben lép életbe, ha nincs európai szintű harmonizált szabályozás. Értelmében, ha egy tagállamban adott terméket jogszerűen forgalmaznak, az más tagállamban is értékesíthető, függetlenül attól, hogy megfelel-e a másik tagállam műszaki szabályainak. A termék forgalomba hozatalának megtagadása egyedül közérdekvédelmen alapulhat.[16]

A kölcsönös elismerés elvének magánjogból bűnügyi együttműködés területére történő átültetése 1998. július 15-16-án a cardiffi Európai Uniós csúcsértekezleten kezdődött, amikor is Jack Straw az Egyesült Királyság belügyminisztere javaslatot terjesztette elő, miszerint az ír, skót és angol jog- és igazságszolgáltatási rendszerben használt kölcsönös elismerés mintájára hozzanak létre Európai szintű bűnügyi együttműködési elvet. A

---

[14] Nánási László: Az európai elfogatóparancs. Scientia Iuris: Román-Magyar Jogtudományi Közlöny, 2012/1-2., 101-102. o. http://jog.sapientia.ro/data/tudomanyos/Periodikak/scientia-iuris/2012-1-2/6.pdf (Letöltve: 2025. 11. 20.).

[15] Uo. 103. o.

[16] European Commission: *Mi a kölcsönös elismerés?* https://tinyurl.com/35nbd6h3 (Letöltve: 2025. 1. 20.).

Tanács a javaslatát elfogadta és következtetéseinek 39. pontjában kimondta annak szükségszerűségét, a már ismertetett tamperei csúcsértekezleten pedig a tagállamok közötti bűnügyi együttműködés alapkövének nevezte. A 39. pontban lefektetett alapok az *Európai Unió működéséről szóló szerződés* (továbbiakban: EUMSZ) *Harmadik részének V. cím 4. fejezetének 82. cikkében* jelennek meg. [17]

A kölcsönös elismerés elvének büntető jogba való átültetését azon felvetés alapozza meg, hogy a tagállamok egységes értékrendszert fogadtak el az Európai Unió megalakításakor és ezen értékrendszer magában foglalja az uniós jog tiszteletben tartását, a közös értékek melletti határozathozatalt. [18] Emellett tagállamok arra alapozva, hogy a több évszázados elkülönült jogfejlődés ellenére egységes alapelveket követnek, illetve arra hogy ugyanazon nemzetközi szervezetek tagjai, ugyanazon emberi jogi egyezmények részesei és alkotmányaikban ugyanazon alapvető demokratikus és jogállamisági elveket érvényesítik kölcsönösen megbíznak egymásban. A tagállamok közötti kölcsönös bizalom fennállta adott lehetőséget egy belső határok nélküli Európai Unió kialakítására és a szorosabb igazságügyi együttműködésre. Ezen alapvető eszme keretében alkották meg az európai elfogatóparancsot, mellyel kapcsolatos gyakorlat indikátora lehet adott tagállam kölcsönös bizalomhoz, közös együttműködéshez fűződő viszonyának.

A kölcsönös elismerés elve alapján a végrehajtó tagállam hatósága nem vizsgálja, hogy a külföldi eljárás megfelelt-e annak az eljárásnak, amelyben azt lefolytatták, hanem csupán azt, hogy összeegyeztethető-e az egyetemes büntetőjogi normákkal.[19]

III. Az európai elfogatóparancs eljárása

Az európai elfogatóparancs kibocsátása az eljárás egyszerűsítése és gyorsítása érdekében, a Kerethatározat mellékletében feltüntetett formanyomtatványon keresztül történik.

Az európai elfogatóparancsnak két típusát különböztethetjük meg: a bíróságnak megfelelő szerv által büntetőeljárás lefolytatásának érdekében és a szabadságvesztés büntetés, illetve szabadságelvonással járó intézkedés végrehajtása céljából kibocsátott elfogatóparancsot. Mindkét esetben a kibocsátás alapját a tagállamban megindult büntetőeljárás jelenti.

Előbbi esetben európai elfogatóparancs olyan cselekmény esetén bocsátható ki, melynél a kibocsátó tagállam joga szerinti büntetési tétel felső határa legalább tizenkét havi szabadságvesztés vagy szabadságelvonással járó intézkedés. Ez esetben az európai elfogatóparancs formanyomtatványához mellékelni kell annak tanúsítását, hogy rendelkezésre áll kibocsátó tagállam általi elfogatóparancs. Az utóbbi kibocsátása akkor

[17] Farkas Ákos: Az Európai Bíróság és a kölcsönös elismerés elvének hatása az európai büntetőjog fejlődésére. *Miskolci Jogi Szemle*, 2011/6., 71-72. o.
[18] Gellér Balázs: Are the Principles of Mutual Trust and Recognition in Danger of Being Eroded by the Recent Jurisprudence of the ECJ Concerning the EAW? *Transnational Criminal Law Review*, 2024/3., 70-71. o.
[19] Uo. 70-71. o.

lehetséges, ha a szabadságvesztést kiszabó ítéletet vagy a szabadságelvonással járó intézkedést már meghozták, időtartama pedig legalább négy hónap. Az európai elfogatóparancs e típusánál szükséges a végrehajtható ítélet vagy más azonos joghatállyal bíró végrehajtható bírósági határozat csatolása is.[20]

A kibocsátást követően – ha ismert helyen tartózkodik a terhelt – az európai elfogatóparancsot a fogadó állam végrehajtó bíróságának megfelelő szervnek címezve megküldik. Az ismeretlen helyen tartózkodó terhelt esetében az európai elfogatóparancs bekerül az SIS (*Schengen Information System)* rendszerbe a SIRENE iroda *(supplementary information request at the national entries)* által. A terhelt elfogását követően a végrehajtó igazságügyi hatóság dönt a végrehajtó tagállam jogával összhangban a fogvatartás fenntartásáról vagy az ideiglenes szabadon bocsátásról, feltéve hogy a hatóság mindent megtett a szökés megakadályozásának érdekében. A végrehajtó igazságügyi hatóság nem vizsgálja az európai elfogatóparancs tárgyát képző bűncselekmény tényállását, a megtagadási okok fennállásának kérdése kapcsán azonban vizsgálatra hivatalból köteles.

Az elfogott személynek lehetősége van beleegyezni az átadásba. Ha nem egyezik bele, joga van a végrehajtó tagállam nemzeti joga szerinti kihallgatáshoz, a végrehajtó igazságügyi hatóságnak pedig hatvan nap áll rendelkezésére az európai elfogatóparancs végrehajtásáról szóló határozat meghozatalára. Ha a terhelt beleegyezik az átadásba, a határozatot tíz napon belül meg kell hozni. A határozat meghozatala után a végrehajtó haladéktalanul értesíti a kibocsátó igazságügyi hatóságot és a lehető leghamarabb, de a határozat véglegessé válásától számított 10 napon belül át kell adnia a keresett személyt.
Érdekesség a hazai átadási eljárásban, hogy a keresett személy a végrehajtó igazságügyi hatóság döntése ellen fellebbezhet, annak viszont a határozat végrehajtására halasztó hatálya nincs. Így megtörténhet, hogy a terhelt átadására – a határozat meghozatalát követő 10 napos határidőn belül - már sor került, annak ellenére, hogy a fellebbviteli bíróság még nem hozott döntést a fellebbezése kapcsán.

III.1. A végrehajtás megtagadása

A kölcsönös bizalom és kölcsönös elismerés elvének megfelelően, korlátozott lehetőség áll rendelkezésre az európai elfogatóparancs végrehajtásának megtagadására. Ezen megtagadási okokat abszolút és relatív kategóriákba sorolhatjuk.

Abszolút megtagadási okok körében a végrehajtó igazságügyi hatóságnak meg kell tagadnia a végrehajtást, ha az európai elfogatóparancs alapjául szolgáló bűncselekmény a végrehajtó tagállamban közkegyelem alá esik és joghatósága van bűncselekmény üldözésére. Továbbá akkor is, ha végrehajtó igazságügyi hatóság rendelkezésére álló információk alapján kiderül, hogy a keresett személyt másik tagállam ugyanazon cselekményért már jogerősen elítélte, és a büntetését már letöltötte, annak végrehajtása folyamatban van, vagy az ítélkező tagállam jogszabályai szerint már nem hajtható végre, illetve ha az európai elfogatóparancs alapján keresett személy a végrehajtó állam

[20] 2002/584/IB tanácsi kerethatározat (2002. június 13.) az európai elfogatóparancsról és a tagállamok közötti átadási eljárásokról.

jogszabályai szerint életkora miatt nem vonható büntetőjogi felelősségre az adott cselekményért. [21]

A felsoroltakon kívül a Kerethatározat 4. cikke hét pontban lehetőséget biztosít az európai elfogatóparancs megtagadásának mérlegelésére. Ezek jellemzően a büntetőeljárás lefolytatásának alapvető akadályai. Nem szükséges végrehajtani például, abban az esetben, ha a végrehajtó tagállam területén az európai elfogatóparancsban megjelölt személlyel szemben ugyanazon cselekmény vonatkozásában – amely az elfogatóparancs alapjául szolgál – büntetőeljárás van folyamatban vagy ha végrehajtó tagállam joga a büntethetőség vagy a büntetés elévülése folytán megszűnt és az érintett cselekmények a végrehajtó tagállam büntetőjoga szerint annak saját joghatósága alá tartoznak.[22]

A nevesített kategóriák mellett, a kerethatározat preambulumából kiolvasható egy általános megtagadási lehetőség, amely kimondja, hogy a Kerethatározat egyetlen rendelkezése sem értelmezhető úgy, hogy az tiltja az olyan személy átadásának megtagadását, akivel kapcsolatban objektív okok alapján feltehető, hogy az elfogatóparancs kibocsátásának a célja, hogy személyét neme, faji vagy vallási hovatartozása, etnikai származása, állampolgársága, anyanyelve, politikai meggyőződése vagy szexuális irányultsága miatti büntetőeljárás alá vonják, illetve ha feltehető, hogy helyzetét bármely említett körülmény hátrányosan befolyásolná.[23]

A kerethatározat külön cikk alatt rendezi az alapvető jogokhoz való viszonyát. Az 1. cikk (3) bekezdése szerint az *Európai Unióról szóló szerződés 6. cikkében* foglalt alapvető jogok és alapvető jogelvek tiszteletben tartásának kötelezettségét a kerethatározat nem érinti, így az eljárás minden szakaszában érvényesülnie kell az idézetben foglaltaknak. Az EUSZ 6. cikkének értelmében az *Emberi Jogok Európai Egyezménye* (továbbiakban: EJEE), az *Európai Unió Alapjogi Chartája* (a továbbiakban: Alapjogi Charta) és a tagállamok közös hagyománya az uniós jogrend részét képző általános elvek. Mindezek értelmében az uniós jognál szigorúbb nemzeti védelmet a tagállamok nem biztosíthatnak, hiszen az összeegyeztethetetlen lenne a kölcsönös bizalom elvével.[24]

Az EUB döntése alapján a tagállamok végrehajtó igazságügyi hatóságainak lehetősége van különleges esetekben az alapvető jogok biztosításának tekintetében az átadás megtagadására. Megtagadható a végrehajtás abban az esetben, ha objektív, megbízható, konkrét bizonyítékok alapján fennáll annak veszélye, hogy a keresett személy átadása ellene irányuló embertelen vagy megalázó bánásmódhoz vezetne a kibocsátó tagállam fogvatartási körülményei okán. Továbbá abban az esetben, ha fennáll annak a valós veszélye, hogy a keresett személy független és pártatlan eljáráshoz való alapvető joga

[21] Uo. 37. o.
[22] Uo. 34. o.
[23] A Bizottság jelentése az Európai Parlamentnek és a Tanácsnak: *az európai elfogatóparancsról és a tagállamok közötti átadási eljárásokról szóló, 2002. június 13-i tanácsi kerethatározat végrehajtásáról.* 3.3. https://eur-lex.europa.eu/legal-content/HU/TXT/HTML/?uri=CELEX%3A52020DC0270 3.3 (Letöltve: 2025. 12. 12.).
[24] Uo. 3.3.

sérülne a kibocsátó tagállam igazságügyi hatóságainak függetlensége kapcsán.[25] Az ezzel kapcsolatos konkrét EUB döntések és azok hatásai később kerülnek kifejtésre.

IV. A kiadatási eljárás és az európai elfogatóparancs közti különbségek

A két jogintézmény különbözősége a tagállamok közt fennálló kölcsönös bizalomból eredeztethető. A kiadatási eljárás a tágabb nemzetközi szinten történő bűnügyi együttműködést előre mozdító eszköz, ami gyakran átpolitizált és ahol az államok a teljes szuverenitásuk birtokában dönthetnek az eljárás végrehajtásáról. Ezzel szemben az európai elfogatóparancs a tagállami igazságügyi hatóságok, önálló és szoros együttműködése, ami eszméjében mentes a politikai befolyástól. Tanulmányom következő fejezetében a már ismertetetteket alapul véve felvázolom a két eljárás közötti legfontosabb különbségeket: a kettős büntethetőséget, politikai befolyástól való mentességet, az állampolgárok kiadatását/átadását, a garanciákat és a megtagadás lehetőségét.

IV.1. Kettős büntetendőség elve

A kiadatási eljárások egyik alapkövét jelentő kettős inkrimináció elvének értelmében vizsgálni kell, hogy a cselekmény *in abstracto* mindkét tagállamban bűncselekménynek minősül-e, illetve hogy adott személy *in concreto* büntethető-e. A megkeresett hatóságnak először ellenőriznie kell, hogy saját jogában fellelhető-e olyan diszpozíció, amelybe a kiadatás alapját képző bűncselekmény beilleszthető. A hatóság a névazonosság helyett az objektív tényállási elemek meglétét vizsgálja. Problémát jelenthet az államok eltérő joggyakorlata a tényállásazonosság kérdésében, hiszen annak szigorúbb értelmezése a kiadatás megtagadásához vezethet.[26]

Az absztrakt szintet követően az eljáró hatóságnak szükséges vizsgálnia a keresett személy büntethetőségének kérdését. Az államok anyagi és eljárásjogi kódexeiben szabályozott büntethetőségi akadályok közül rendszerint azon eseteket kell szemügyre venni, amelyek nem igénylik a bizonyítékok mérlegelését és függetlenek a terhelt szubjektumától. Ezek az úgynevezett nevesített kooperációs akadályok, mint például az elévülés és a kegyelem.[27]

Az európai elfogatóparancs esetében az egyre szorosabb, büntetőügyekben folytatott igazságügyi együttműködés következtében, illetve a kölcsönös bizalom elvéből valamint a közös értékrendszerből adódóan az Európai Unió tagállamai harminckét bűncselekmény esetében lemondtak a kettős büntetendőség feltételéről, ha a kibocsátó tagállam joga szerint a büntetési tétel felső határa legalább háromévi szabadságvesztés vagy szabadságelvonással járó intézkedés. A felsorolt bűncselekmények tárgyi súlyuk és a már

[25] European Commission: *European arrest warrant statistics report 2022.* 22. o. https://tinyurl.com/mr5bt5n7 (Letöltve: 2025. 11. 20.).
[26] M. Nyitrai 2003: i.m. 80. o.
[27] M. Nyitrai 2003: i.m. 83-84. o.

létező jogharmonizáció következtében váltak a kerethatározat részévé, ilyenek például terrorizmus vagy az emberkereskedelem. [28]

A fel nem sorolt bűncselekmények esetén az európai elfogatóparancs végrehajtásának feltételéül szabható, hogy a keresett személy által elkövetett cselekmény a végrehajtó tagállam jogrendszere szerint – a tényállás részleteire vagy a cselekmény jogi minősítésére tekintet nélkül – bűncselekménynek számítson. [29]

A kettős inkrimináció célja, hogy tekintettel az államok évszázadokon át kialakult eltérő jogfelfogására, lehetőséget biztosítson a kiadatás megtagadására.[30] Ezen túlmenően természetéből adódóan kimagasló szerepet játszott a tagállamok közti – továbbra is fennálló – kriminalizációs különbségek kiküszöbölésében. A terhelti jogok efféle jellegű védelmére a hatályos büntető-normarendszerünkben is szükség van, hiszen a belső határok eltörlése lehetővé tette az uniós polgárok számára, hogy állampolgárságuk megtartása mellett életvitelszerűen tartózkodjanak más tagállamban, ahol olyan munkát vállalhatnak, olyan gazdasági tevékenységet folytathatnak és olyan magatartást valósíthatnak meg melyek nem összeegyeztethetők személyes joguk szerinti tagállam büntető normáival. Ily módon elképzelhető, hogy egy magyar állampolgár Belgiumban eutanázia teljesítésében nyújt segítséget belga barátjának, mely által megvalósítja a *büntető törvénykönyvről szóló 2012. évi C. törvény* 162. § (1) bekezdése szerinti öngyilkosságban közreműködés bűntettét.

Ehhez hasonló esetek komoly aggályokat vethetnek fel, tekintettel arra, hogy jelen esetben nem csupán a magyar állampolgárral szemben, de az eutanáziát teljesítő egészségügyi dolgozókkal szemben is helye lenne európai elfogatóparancs kibocsátásának. Mindezek tükrében megállapítható, hogy a kettős inkrimináció elvének áttörése a tagállamok közötti bűnüldözés szempontjából kiemelkedő jelentőségű. Ugyanakkor az uniós jogalkotó és egyben a tagállamok számára nem elhanyagolandó az abból származó konfliktusok megoldása, ha valóban egy a szabadságon, a biztonságon és a jog érvényesülésén alapuló térség kialakítását szeretnék elérni.

IV.2. Politikai befolyástól való mentesség

A Kiadatási Egyezmény 3. cikkében találhatóak az úgynevezett politikai bűncselekmények. Az egyezmény nem tartalmaz taxatív felsorolást, hanem lehetőséget biztosít a részes államoknak annak mérlegelérésre, hogy a bűncselekmény – ami miatt a keresett személy kiadatását kérik – politikai bűncselekménynek vagy politikai bűncselekménnyel összefüggő bűncselekménynek minősül-e. Tovább tágítja a fogalom értelmezési körét a 3. cikk (2) bekezdése mivel – mint az első esetben – nem engedélyezik a kiadatást abban az esetben, ha alapos okkal feltételezhető, hogy a

[28] Gellér Balázs: A kölcsönös elismerés elvén alapuló bűnügyi együttműködés. In: Hollán Miklós (szerk.): Az EU mint a szabadság, a biztonság és a jog térsége. Magyarország az Európai Unióban 2004–2014. NKE Nemzetközi Intézet, Budapest, 2014, 95. o.
[29] Lásd: 18. lj. 2. cikk (2) bekezdés.
[30] Bátki Pál: *Miben különbözik az európai elfogatóparancs alapján történő átadás a kiadatástól?* https://jogaszvilag.hu/szakma/miben-kulonbozik-az-europai-elfogatoparancs-alapjan-torteno-atadas-a-kiadatastol/ (Letöltve: 2025.12.12.).

kiadatási kérelmet köztörvényi bűncselekményre hivatkozva azért terjesztették elő, hogy az érintett személlyel szemben faji, vallási, nemzetiségi hovatartozása vagy politikai nézetei miatt büntetőeljárást indítsanak, büntetést szabjanak ki, illetve hogy e tényezők bármelyike következtében hátrányosabb elbánásban részesüljön. Mindez lehetőséget biztosít az végső döntést meghozó kompetens hatóság számára, hogy politikai alapon megtagadja a kiadatás végrehajtását.[31]

Az európai elfogatóparancs esetében a miniszteriális szint, döntési jogkörrel nem rendelkezik. A végrehajtó állam igazságügyi hatóságai bírálnak el minden lényeges kérdést önállóan és befolyástól mentesen. Nem számít a keresett személy által elkövetett bűncselekmény politikai vonzata, egyedül a kerethatározat által biztosított megtagadási okok vehetők figyelembe.[32]

IV.3. Saját állampolgárok kiadatása és átadása

Az Kiadatási Egyezmény még lehetővé tette a saját állampolgárok kiadatásának megtagadását. A megtagadás lehetősége mellett szólt a részes államok egymás jogrendszeréhez fűzött kölcsönös bizalmatlansága, továbbá azon felvetés, hogy a terhelt leghatékonyabban saját állampolgársága szerinti országban képes védekezni. A Kerethatározat elfogadásával mindez már alaptalanná vált, hiszen a tagállamok folyamatos jogharmonizációja és együttműködése lehetővé tette a kölcsönös bizalom fennállását, valamint a kölcsönös elismerés elvének büntetőügyekbe való átültetését.[33] A hatékony védekezés biztosítására a tagállamok megfelelő szabályokat hoztak létre eljárásjogi kódexeikben, ilyen például az anyanyelvhasználathoz való jog.

IV.4. Garanciák

Mind a kiadatás, mind pedig az átadás esetén felfedezhetünk garanciákat. A Kiadatási Egyezményben a 11. cikk szabályozza a halálbüntetés esetében nyújtható biztosítékot. Ez esetben megtagadható a kiadatás, ha azt olyan bűncselekmény miatt kérik, amely a megkereső állam joga szerint halálbüntetéssel sújtható, de a megkeresett állam jogrendszere nem alkalmazza ezt a jogintézményt vagy általában nem hajtja végre. Kivételt jelent, ha a megkereső állam olyan biztosítékot nyújt, amely garantálja, hogy a halálbüntetést nem fogják végrehajtani.[34]

Az európai elfogatóparancs esetében a végrehajtás feltételhez kötése három esetben lehetséges. Ha az európai elfogatóparancsot olyan ítélet végrehajtása miatt adták ki, amelyet a terhelt távollétében hoztak meg, és őt személyesen nem idézték be, valamint a tárgyalás időpontjáról és helyéről más módon nem értesítették, akkor az átadás annak feltételhez köthető, hogy a kibocsátó ország biztosítékot ad arra, hogy az illető kérheti az ügy újratárgyalását és a tárgyaláson való jelenlétét. Az érintett személy átadása továbbá azon feltételhez köthető, ami biztosítja annak lehetőségét, hogy ha a vele szemben életfogytiglan tartó szabadságvesztés - büntetést szabnak ki, akkor meghatározott idő elteltével jogosulttá váljon felülvizsgálat kérelmezésére. Végül pedig, ha a terhelt a

[31] Európai Kiadatási Egyezmény 3. cikk.
[32] Bátki: i.m.
[33] M. Nyitrai 2003: i.m. 141. o.
[34] Lásd: 30. lj. 11. cikk.

végrehajtó tagállam állampolgára vagy lakosa, lehetséges azon feltétel kikötése, ami a kiszabott szabadságvesztés büntetés végrehajtó tagállamban letöltését garantálja.[35]

A kiadatási eljárástól eltérően az európai elfogatóparancs feltétel-kikötési szabályai nem alapvető jogok érvényesülésével kapcsolatosak, hanem az eljárás jogszerűségével, illetve a már kiszabott büntetés végrehajtásával. Egyéb feltétel megállapítása nem lehetséges, hiszen összeegyeztethetetlen lenne a kölcsönös elismerés elvével.

IV.5. Megtagadási okok szűkítése

Az európai kiadatási egyezmény hét nevesített megtagadási lehetőséget biztosít a tagállamok számára: politikai bűncselekmények, katonai bűncselekmények, pénzügyi bűncselekmények, saját állam kiadatása, az elkövetés helye, folyamatban lévő eljárás ugyanazon bűncselekmény miatt, non bis in idem, elévülés és halálbüntetés. A felsoroltak tartalmaznak általánosnak mondható elveket, mint az elévülés vagy a non bis in idem, ugyanakkor tág bűncselekményi kört is, ahol lehetőség adódik a megkeresett állam számára, hogy mérlegelje a keresett személy kiadatását. Az egyezmény továbbá kizár bizonyos bűncselekményeket a kiadatási eljárásból, ilyenek például egyes katonai bűncselekmények.[36]

Az európai bűnügyi együttműködés következtében a megtagadási okok köre, az európai elfogatóparancsról szóló kerethatározatban gyakorlatilag a büntetőeljárás lefolytatásának, valamint végrehajtásának akadályaira - különös esetben körülményeire -, továbbá a hatékonyságnak és célszerűségnek biztosítására szűkült.

V. Az európai elfogatóparancs eredménye

A Kerethatározat célkitűzése a hosszadalmas kiadatási eljárások egyszerűsítése és gyorsítása volt, ezért szigorú határidőket, bizonyos esetekben pedig soron kívüliséget állapított meg annak érdekében, hogy az átlagosan egy évig tartó kiadatást lerövidítse.[37]

A tagállamok sajnos nem minden esetben ültették át egyértelműen nemzeti jogukba a Kerethatározat rendelkezéseit. A keresett személy beleegyezését követő tíz napon belüli döntéshozatali határidőt két tagállam sem ültette át, a belegyezés megtagadása esetére vonatkozó hatvannapos határidőt pedig több tagállam helytelenül ültette át vagy azt egyáltalán nem tette meg. Továbbá a tagállamok többségének belső jogában nem található meg azon rendelkezés, amely az említett határidők harminc napos meghosszabbítása esetén tájékoztatási kötelezettséget ír elő a végrehajtó igazságügyi hatóságnak.[38]

---

[35] Európai igazságügyi portál: *Európai elfogatóparancs.* https://e-justice.europa.eu/topics/court-procedures/criminal-cases/judicial-cooperation/european-arrest-warrant_hu (Letöltve: 2025.12.12.).
[36] Európai Kiadatási Egyezmény 3-11. cikk.
[37] Nánási: i.m. 112. o.
[38] Lásd: 22. lj.

Az európai elfogatóparancs alkalmazására vonatkozó statisztikai adatok alapján 2018 és 2022 között hozzájárulás esetén 16,4-21,25 napon belül történt meg a körözött személyek átadása, hozzájárulás nélkül 45-72,45 napra tehető az eljárás hossza. Az átlag természetesen nem mutatja a tagállamok közötti eltéréseket. Hozzájárulás megtagadása esetén 2022-ben Litvánia 43 nap alatt, Szlovákia 42 nap alatt, Írország 41 nap alatt teljesítette az átadást nagyban meghaladva a főszabály szerinti 10 napos határidőt. Hozzájárulással Írország 309 nap alatt, Szlovákia 101 nap alatt, a többi tagállam átlagosan 60 nap alatt hajtotta végre a kérelmet, a kirívó eseteket kivéve a maximum 90 napos határidőn belül.[39] A bizottság jelentése szerint az átadás végrehajtásának elhúzódása a hosszadalmas fellebbezési eljárásoknak tudható be. Az ismertetettek alapján meg kell állapítanunk, hogy a Kerethatározat legfőbb célkitűzését elérte, hiszen a keresett személyek átadása átlagban kevesebb mint 2 hónapra rövidült.

Érdekesen alakult a kibocsátott és végrehajtott európai elfogatóparancsok aránya. 2014-től 2018-ig folyamatosan nőtt a kibocsátások és a végrehajtások száma, mindig szinte egyharmados arányban. 2019-ben a kibocsátott elfogatóparancsok száma elérte eddigi csúcsát 20.226-ot, a végrehajtottak száma azonban megmaradt az átlagosnak mondható ötezer körül, a vizsgált évben pontosan 5.665. Jelenleg a kibocsátott európai elfogatóparancsok száma csökkenő tendenciát mutat és 2022-ben elérte az eddigi legalacsonyabb mértékét 13.335-vel, míg a végrehajtottak továbbra is átlagon belülinek mondhatók. A drasztikus csökkenés oka, hogy 2019-ben 2.379 európai elfogatóparancsot a német ügyészség bocsátott ki, melyeket le kellett vonni, azonban még így is megállapítható a kibocsátások csökkenése.[40]

A nem teljesített európai elfogatóparancsok legnagyobb része 34%, a Kerethatározat 4. cikkének (6) bekezdésén alapul, azaz a megtagadás oka, hogy a végrehajtó tagállamban történjen a szabadságvesztés-büntetés vagy szabadságvesztéssel járó intézkedés kitöltése. Az átadások 11%-át tagadták meg egyes mérlegelhető okokra hivatkozva, tehát többek között a végrehajtó tagállamban ugyanazon cselekmény miatt folyamatban lévő büntetőeljárásra hivatkozva. Szintén 11%-a származik olyan határozatok végrehajtásának megtagadásából, amelyeket olyan tárgyaláson hoztak, amelyeken az érintett személy nem volt személyesen jelen és további 11% „más” okra alapítva nem kerül végrehajtásra. Fontos kiemelni, hogy a kibocsátott európai elfogatóparancsok 6%-nak teljesítését tagadják meg a végrehajtó igazságügyi hatóságok a Kerethatározat 1. cikkének (3) bekezdésére, az alapvető jogokra alapozva. Ezen 6% magába foglalja az alapvető jogok széles körét, így például megtagadási okként szolgálhat a magán- és a családi élet tiszteletben tartásának joga. A Kerethatározat 1. cikkének (3) bekezdése ugyanakkor tartalmaz olyan alapvető jogokat, melyek tagállami megsértése, elégtelen teljesítése vonja maga után a végrehajtás megtagadását.[41]

VI. Az Európai Unió Bíróságának releváns gyakorlata

[39] Lásd: 24. lj. 7. o.
[40] Uo. 7. o.
[41] Uo. 7. o.

Az utóbbi évtizedben az európai elfogatóparanccsal kapcsolatban kialakult Bírósági gyakorlat aggályossá teheti a jogintézmény és a kölcsönös elismerés elvének jövőjét. A Kerethatározat pontosan meghatározza a végrehajtás megtagadásának lehetőségeit, az EUB ugyanakkor az alapvető jogok tiszteletben tartásának okán lehetőséget biztosított a kérelem teljesítésének megtagadására. Mint láthattuk a tagállamok végrehajtó igazságügyi hatóságai számottevő esetben alkalmazták ezt az alternatívát, ami aggodalmat vet fel a kölcsönös elismerés elvének érvényesülésével kapcsolatban. Az erre vonatkozó legfontosabb Bírósági határozatokat szeretném az alábbiakban ismertetni.

VI.1. Aranyosi és Căldăraru C-404/15 és C/659/15 PPU. (2016)

A magyar bíróság 2014. november 4-én elfogatóparancsot bocsátott ki Aranyosi P.-vel szemben büntetőeljárás lefolytatásának céljából. R. Căldăraru román állampolgár iránt 2015. október 29- én bocsátottak ki európai elfogatóparancsot szabadságvesztés-büntetés végrehajtásának céljából. Mindkét személyt Németországban fogták el és mindkét személy esetében az Brémai Tartományi felsőbíróság vizsgálta az átadás feltételeinek fennállását. A német bíróság megállapította, hogy egyik esetben sem lehetséges abszolút vagy relatív megtagadási ok alapján az európai elfogatóparancs teljesítésének megtagadása. Ugyanakkor a brémai bíróság döntése szerint az 1982. december 23- i a *nemzetközi bűnügyi jogsegélyről szóló törvény* (IRG) 73. § alapján átadási akadály áll fenn, mivel megalapozott annak a gyanúja, hogy a magyar és román igazságügyi hatóságnak történő átadás esetén az említett személyek olyan fogvatartási körülmények közé kerülhetnek, amelyek sértik az EJEE 3. cikke szerinti alapvető jogokat és az EUSZ 6. cikke szerinti általános elveket. Mindezt alátámasztotta Emberi Jogok Európai Bíróságának (továbbiakban: EJEB) 2015. március 10-i Varga és társai kontra Magyarország ítélete, valamint a 2014. június 10-i Romániát marasztaló ítélete. Határozataiban az EJEB mindkét tagállam esetében megállapította, hogy börtöneik túlzsúfoltsága, valamint a szűk és piszkos cellák miatt megsértették a fogvatartottak alapvető jogait. [42]

A Bíróság a két ügy kapcsán kidolgozta az úgynevezett „Aranyosi tesztet", mely alapján objektív feltételek fennállása esetén visszautasítható az európai elfogatóparancs végrehajtása. A teszt értelmében vizsgálandó, hogy a kibocsátó tagállamban a fogvatartási körülményekkel kapcsolatban objektív, megbízható, konkrét és megfelelően naprakész bizonyítékok állnak-e rendelkezésre, amelyek bizonyítják, hogy rendszerszintű hiányosságok állnak fenn. Ezen általános vizsgálatot követően szükséges a végrehajtó igazságügyi hatóságnak ellenőriznie, hogy az érintett személy esetében alapos okkal feltételezhető-e, hogy fogva tartásának feltételei miatt embertelen vagy megalázó bánásmódban részesülhet.[43]

Fontos kiemelni, hogy a feltételek megállapítása érdekében az EUSZ 4. cikk (3) bekezdés szerinti lojális együttműködésre alapozva a kerethatározat 15. cikk (2) bekezdése szerint a végrehajtó igazságügyi hatóság tájékoztatást köteles kérni a kibocsátó tagállamtól. Ezt

[42] C-404/15. és C-659/15. PPU. Aranyosi és Căldăraru ECLI:EU:C:2016:198. 28-45. bekezdés.
[43] Uo. 105.bekezdés.

követően az információk továbbításáig elhalasztja a határozathozatalt, majd a szükséges adatok megérkezése után dönt az átadásról.[44]

A Bíróság döntésének értelmében, amennyiben az Aranyosi tesztben foglalt feltételek fennállnak a végrehajtó igazságügyi hatóságnak fel kell függesztenie a határozathozatalt, mindaddig, amíg kézhez nem kapja azokat az információkat, melyek alapján megalapozott döntést hozhat a kifogásolt körülmények tényleges fennállásáról. Abban az esetben, ha a veszély ésszerű időn belül nem zárható ki, a végrehajtó hatóságnak döntenie kell az eljárás megszüntetéséről. Az EUB ítéletével lehetővé tette a terhelt alapvető jogainak védelmét amellett, hogy megtartotta a jogintézmény létjogosultságát, hiszen nem tette lehetővé a alapjogok sértésén alapuló automatikus elutasítást, ami az európai elfogatóparancs és a kölcsönös elismerés elvének rendeltetésével ellentétes.[45] Ugyanakkor az Európai Unió kölcsönös együttműködésének elvéből fakad, hogy bármely tagállam ugyanazon feltételeket képes biztosítani saját hatóságai előtt. Természetesen a gyakorlatban ez eltér, jelen esetben a fogva tartási körülményekben. Kérdéses, hogy a probléma megoldása az a megtagadási okok bővítése valamint a kötelező felfüggesztés alkalmazása és ezzel összefüggésben a kölcsönös elismerés elvének csorbítása, vagy például a tagállamok büntetés-végrehajtási intézeteinek uniós szintű ellenőrzése, forrásokkal való támogatása.

Kiemelendő, hogy a határozathozatal felfüggesztése és az objektív jól behatárolt információk alapján való döntéshozatal és ezáltal az eljárás lassítása, bonyolultabbá tétele még nem értékelhető a kiadatás intézményéhez való visszatérésként. Viszont a végrehajtó igazságügyi hatóság információ beszerzési kötelezettsége már igen, hiszen az európai elfogatóparancs és a kölcsönös elismerés elvének magjában a tagállamok között fennálló bizalom áll, mely alapján sajátjuktól eltérő intézményrendszer vizsgálata szükségtelennek minősül. A Bíróság az ítéletében nem ment odáig, hogy végrehajtó igazságügyi hatóság garanciákat kérhessen a kibocsátó tagállamtól, az már vita nélkül hátralépésként lenne értékelhető.

VI.2. LM C-216/18 PPU. (2018)

A lengyel bíróságok három alkalommal bocsátottak ki európai elfogatóparancsot LM-el szemben büntetőeljárás lefolytatásának céljából, mivel fennállt annak gyanúja, hogy kábítószerek és pszichotróp anyagok jogellenes kereskedelmének bűncselekményét követte el. LM-et az ír hatóságok elfogták és a felső bíróság elé állították, ami Lengyelországnak való átadásához nem járult hozzá. Döntését azzal indokolta, hogy átadása az EJEE 6. cikkébe ütközne és az igazságszolgáltatás kirívó megtagadásának veszélyének tenné ki, mivel a lengyelországi jogalkotási reformok megfosztják a tisztességes eljáráshoz való jogától. LM hivatkozott az Európai Bizottság (továbbiakban: Bizottság) lengyelországi jogállamisággal kapcsolatban 2017. december 20. napján

[44] Uo. 105. bekezdés.
[45] Koósné dr. Mohácsi Barbara: *A túlzsúfolt börtönök hatása az európai elfogatóparancs végrehajtására.* https://jogaszvilag.hu/vilagjogasz/a-tulzsufolt-bortonok-hatasa-az-europai-elfogatoparancs-vegrehajtasara/ (Letöltve: 2026.03.25.).

elfogadott indoklással ellátott javaslatára, mely részletezi a bíróságok függetlenségével kapcsolatos aggályokat.[46]

Az EUB hangsúlyozza a kölcsönös elismerés jelentőségét a büntetőügyekben folytatott igazságügyi együttműködés terén, ugyanakkor megerősíti és kibővíti az Aranyosi és Căldăraru ügyben kidolgozott teszt alkalmazási körét. A bíróság döntése alapján a Kerethatározat 1. cikkének (3) bekezdését a következőképp kell értelmezni: *„Amennyiben a büntetőeljárás lefolytatása céljából kibocsátott európai elfogatóparanccsal érintett személy átadásáról dönteni hivatott végrehajtó igazságügyi hatóság olyan bizonyítékokkal rendelkezik, mint amelyek a Bizottság által az EUSZ 7. cikk (1) bekezdése alapján elfogadott indokolással ellátott javaslatban szerepelnek, amelyek alkalmasak annak alátámasztására, hogy a kibocsátó tagállam igazságszolgáltatásának függetlenségét érintő rendszerszintű vagy általános hiányosságok okán fennáll a Charta 47. cikkének második bekezdésében biztosított tisztességes eljáráshoz való alapvető jog megsértésének valós veszélye, akkor az említett hatóságnak konkrétan és pontosan értékelnie kell, hogy – e személynek a személyes helyzetére, valamint az eljárás alapjául szolgáló bűncselekmény jellegére és az európai elfogatóparancs ténybeli hátterére tekintettel, illetve az említett kerethatározat 15. cikkének (2) bekezdésének megfelelően a kibocsátó tagállam által szolgáltatott információkra figyelemmel – komoly és bizonyítékokkal alátámasztott okokból vélelmezhető-e, hogy az érintett személy az e tagállamnak történő átadása esetén ennek a veszélynek ki lenne téve”*.[47]

Mindezek szerint megállapítható, hogy az EUB hármas szintű vizsgálati eljárást dolgozott ki a tagállami igazságügyi rendszerek függetlenségének megállapítására. Első lépésként szükséges az általános teszt lefolytatása, ami az általános és rendszerszintű hiányosságok feltárását célozza. Ezt követi a köztes teszt elvégzése, ami megállapítja a hiányosságok hatásának mértékét. Az első két teszt negatív eredményéből nem következik szükségszerűen az elfogatóparancs megtagadása, ugyanis az nem feltétlenül idézi elő az érintett személy tisztességes eljáráshoz való jogának sérelmét. Ennek értelmében el kell végezni az keresett személyre vonatkozó egyéni tesztet, ami konkrétan megállapítja jogsértést.[48]

Az EUB megerősítette és tovább fejlesztette az Aranyosi és Căldăraru ügyben kidolgozottakat, hiszen mindkét ügyben objektív, megbízható és pontos bizonyítékok alkalmazására kötelezte a végrehajtó igazságügyi hatóságot továbbá előírta, hogy a lojális együttműködés elve alapján egyéb, a kibocsátó tagállamtól származó információkkal is támassza alá döntését. A két ítélet, ugyanakkor elkezdte megváltoztatni az európai elfogatóparancs eszméjét, mivel más intézmények jelentéseihez kötve lehetővé tették a

[46] C-216/18. PPU. Minister for Justice and Equality kontra LM ECLI:EU:C:2018:586.
[47] Uo. 79. bekezdés.
[48] Stanisław Biernat – Paweł Filipek: The Assessment of Judicial Independence Following the CJEU Ruling in C-216/18 LM. In: Armin von Bogdandy et al. (eds): *Defending Checks and Balances in EU Member States: Taking Stock of Europe's Actions.* Springer, Berlin, 2021, 418. o.

végrehajtó igazságügyi hatóságoknak más tagállamok létesítményeinek és jogállamiságának vizsgálatát.[49]

VI.3. X.Y. C-562/21 PPU. és C-563/21 PPU. (2022)

A lublini regionális bíróság 2021. április 6. napján európai elfogatóparancsot bocsátott ki annak érdekében, hogy állampolgárukkal szemben 2020. június 30. napján jogerős ítéletben kiszabott két év szabadságvesztés-büntetést végrehajtsák. A keresett személyt a holland hatóságok elfogták, aki az átadásába nem egyezett bele. A holland bíróság az európai elfogatóparancs kapcsán előzetes döntéshozatali eljárást indított.[50]

Az előterjesztő bíróság álláspontja szerint a 2017. december 8-i a *nemzeti igazságszolgáltatási tanácsról szóló törvény és egyéb törvények módosításáról szóló törvény* és különösen a nemzeti igazságszolgáltatási tanács (KRS*)* által kinevezett, az igazságszolgáltatásban részt vevő személyek sérthetik a keresett személy tisztességes eljáráshoz való jogát. Feltételezését a lengyelországi legfelsőbb bíróság 2020. január 23-i állásfoglalására alapozta, ahol megállapították, hogy a KRS politikai hatóságok alá tartozik és így függetlenségét elvesztette, melynek következtében hiányosságok léptek fel a bírák kinevezésének eljárásában. Az előterjesztő bíróság álláspontja szerint mindez ellentétes az Alapjogi Charta 47. cikkével és az EJEE 6. cikkével. A bíróság továbbá megállapította, hogy 2019. december 20-i *a rendes bíróságok szervezetéről szóló törvény, a legfelsőbb bíróságról szóló törvény és egyes más törvények módosításáról szóló törvény* értelmében az érintett személy nem vitathatja a bírák kinevezésének érvényességét és az igazságszolgáltatási feladataik ellátásának jogszerűségét. A Zielona Góra-i lengyel regionális bíróság által 2021. április 7. napján kibocsátott európai elfogatóparancs végrehajtásáról szintén az említett holland bíróság volt jogosult dönteni. Az előterjesztő bíróság az ismertetekkel egyezően indokolt.[51]

Az Európai Unió bíróságának abban a kérdésben kellett döntenie, hogy mely szempontokat kell alkalmaznia a szabadságvesztés-büntetés vagy szabadságelvonással járó intézkedés végrehajtása céljából kibocsátott elfogatóparancs teljesítésekor a végrehajtó igazságügyi hatóságnak, amikor is azt vizsgálja, hogy a kibocsátó tagállamban az ítélethez vezető eljárás során sérült-e a törvény által megelőzően létrehozott bírósághoz való jog, ha e tagállamban e jog megsértése esetében nem áll rendelkezésre hatékony jogorvoslat.[52]

A Bíróság döntése alapján a Kerethatározat 1. cikkének (2) és (3) bekezdését akként kell értelmezni, hogy az átadásról dönteni jogosult igazságügyi hatóság, ha olyan információkkal rendelkezik, amelyek a kibocsátó tagállam igazságszolgáltatásának függetlenségre, valamint a bírói hatalom tagjainak kinevezésére vonatkozó eljárást érintő

[49] Gellér 2024: i.m. 78-79 o.
[50] C-562/21. PPU. és C-563/21. PPU. X és Y kontra Openbaar Ministerie ECLI:EU:C:2022:100 9-31. bekezdés.
[51] Uo. 39. bekezdés.
[52] Uo. 20-21. bekezdés.

rendszerszintű vagy általános hiányosságokra utalnak, akkor két esetben megtagadhatja a keresett személy átadását:[53]

(I) Szabadságvesztés-büntetés vagy szabadságelvonással járó intézkedés végrehajtása céljából kibocsátott európai elfogatóparancs megtagadható, ha a végrehajtó igazságügyi hatóság megállapítja, hogy az ügy körülményei szerint komoly és bizonyítékokkal alátámasztott okokból vélelmezhető, hogy a keresett személy Alapjogi Charta 47. cikke szerinti jogai sérültek. Ilyen bizonyítéknak minősül különösen az érintett személy által az eljáró testületről rendelkezésre bocsátott információ, illetve a pártatlanság és függetlenség megállapítását elősegítő bármely bizonyíték.[54]

(II) Büntetőeljárás lefolytatása céljából kibocsátott európai elfogatóparancs abban az esetben, ha a végrehajtó igazságügyi hatóság megállapítja, hogy a konkrét ügy körülményei szerint komoly és bizonyítékokkal alátámasztott okokból vélelmezhető, hogy az érintett személy esetében fennáll annak valós veszélye, hogy átadása esetén alapvető jogai sérülnek. Ezen körülmény bizonyítására szolgál különösen az érintett személy által nyújtott személyes helyzetével, büntetőeljárás alapjául szolgáló bűncselekmény jellegével, az európai elfogatóparancs kibocsátásának ténybeli hátterével kapcsolatos információ, továbbá bármely más körülmény és bizonyíték, amely releváns az ítélkező testület függetlenségének és pártatlanságának megállapításához.[55]

A döntés kapcsán felmerül a kérdés, hogy az milyen hatással van a kölcsönös elismerés elvére? Az EUB az LM ügyhöz hasonlóan tovább bővítette az európai elfogatóparancs megtagadásának lehetőségét, viszont jelen esetben a végrehajtás megtagadását nem „külső" intézmények által lefolytatott eljárás eredményeként létrejött információkhoz kötötte, mint például a Bizottság indoklással ellátott javaslata, hanem egy általános bizonyíték fogalomhoz. Ezen bizonyíték származhat különösen az érintett személytől, de érdekesebb, hogy az EUB felruházta a végrehajtó igazságügyi hatóságokat a kibocsátó tagállam bíróságainak, büntetés-végrehajtási intézeteinek és az elfogatóparancs tárgyát képző bűncselekménnyel kapcsolatos büntetőeljárásának vizsgálatára. A végrehajtó igazságügyi hatóság efféle jogosultsága alapvetően ellentétesnek mondható a kölcsönös elismerés elvével, hiszen annak az a célja, hogy a tagállamok közötti bizalomra alapozva – az alaki elemeket kivéve – vizsgálat nélkül elfogadják más tagállamok határozatait.[56]

VI.4. C-819/21. Staatsanwaltschaft Aachen (2023)

A lengyel *szczecin-prawobrzeżei* kerületi bíróság 2018. augusztus 7-én hat hónap szabadságvesztésre ítélte MD-t. A büntetés végrehajtását eredetileg felfüggesztették, az ezzel kapcsolatos végzést a bíróság később visszavonta és a szczecini regionális bíróság európai elfogatóparancsot bocsátott ki, ami alapján MD-t Németországban letartóztatták. A német végrehajtó igazságügyi hatóság viszont megtagadta annak teljesítését, mivel MD szokásos tartózkodási helye Németországban található, ezért a lengyel bíróság kérte a kiszabott szabadságvesztés-büntetés végrehajtását. A német bíróság előzetes

[53] Uo. 103. bekezdés.
[54] Uo. 103. bekezdés.
[55] Uo. 103. bekezdés.
[56] Gellér 2024: i.m. 79-80. o.

döntéshozatal iránti kérelmet terjesztett elő, melyben aggodalmát fejezte ki MD tisztességes eljáráshoz való joga kapcsán, mivel úgy ítélte meg, hogy a jogállamiság és a lengyel igazságszolgáltatás függetlensége terén általános hiányosságok mutatkoznak.[57]

A Bíróság döntése megerősítette az X.Y. ügyben hozott változásokat. Az ítélet nem boncolja tovább az információ és bizonyíték fogalmát, hanem az LM ügyben pontosított Aranyosi teszt megfelelő alkalmazását taglalja. A Bíróság továbbra is lehetővé teszi a tagállamok végrehajtó igazságügyi hatóságainak az információk tág körének alkalmazását a rendszerszintű vagy általános hiányosságok megállapítása érdekében. Következésképpen a döntés változást nem hozott, hanem tovább erősíti az előző évben történt paradigmaváltást.[58]

A fentiek alapján arra a következtetésre juthatunk, hogy a jövőbeni ítélkezési gyakorlatban – így például a C-722/23. és C-91/24. sz. egyesített ügyekben (Rugu és Aucroix) – a Bíróság fenntartja az alapjogok védelmének jelenlegi kereteit és nem várható a kölcsönös elismerés elvének megerősítése.[59]

VI.5. Következtetések

Az ismertetettek alapján úgy vélem megállapítható, hogy az EUB mérlegre helyezte az emberi jogok valamint a jogállamiság érvényesülését a kölcsönös elismerés elvével. Az EUSZ 2. cikkének értelmében az Európai Unió az emberi méltóság tiszteletben tartása, a szabadság, a demokrácia, az egyenlőség, a jogállamiság valamint az alapvető jogok tiszteletben tartásának értékein alapul. Ezen elvek érvényre juttatását képviseli nemzetközi szintű fellépése folyamán, valamint a közös politika és tevékenység meghatározása és végrehajtása során, így szükséges azok megjelenése az Unió által kidolgozott bűnügyi együttműködési eljárások alatt is. Az Aranyosi és Căldăraru, valamint az LM ügy lehetőséget biztosítottak az alapvető jogok érvényre jutásának, a kölcsönös elismerés elvének túlzott megszorítása nélkül, hiszen a tagállami végrehajtó igazságügyi hatóság a döntését más, minden tagállam által elismert és részes intézmények jelentéseihez kötötte. A végrehajtó igazságügyi hatóságok döntésének ilyen jellegű keretek közé szorítása gyakorlatilag nem ad lehetőséget a mérlegelésen alapuló határozathozatalnak. Ezzel szemben az X.Y. ügyben az EUB lehetővé tette a végrehajtó igazságügyi hatóságok számára, hogy az érintett személy által szolgáltatott és egyéb bizonyítékok alapján mérlegeljék más tagállamok alapvető jogoknak való megfelelését és ez által értékítéletet mondjanak a kibocsátó igazságügyi hatóság intézményrendszere felett. Az EUB ezen döntésével megtörte saját, addig kialakított gyakorlatát, ami az európai bűnügyi együttműködés képében úgy is értékelhető, mint a kiadatási eljárásba való visszalépés, hiszen ismét bekerült néhány eleme az átadási eljárásba.

A kiadatási eljárás fajsúlyos jellemzője a végső miniszteriális szintű döntés, ezzel szemben az európai elfogatóparancs igazságügyi hatóságok közötti bűnügyi együttműködés, ami a kölcsönös bizalom elvén nyugszik. A végrehajtó igazságügyi

[57] Nicholas Emiliou főtanácsnok indítványa: C-819/21. sz. ügy. Ismertetés napja: 2023. május 4..
[58] C-819/21. Staatsanwaltschaft Aachen ECLI:EU:C:2023:841.
[59] Athanasios Rantos főtanácsnok indítványa: C-722/23. és C-91/24. sz. egyesített ügyek. Ismertetés napja 2025. július 10..

hatóság döntése akaratlanul is politikai irányba tereli az eljárás megítélését, ha annak alapja a kibocsátó igazságügyi hatóság jogállamisághoz fűződő viszonya. Nem különbözne ettől az sem, ha a végrehajtó igazságügyi hatóságnak az embertelen bánásmód vagy körülmények fennállásáról kéne dönteni. Ennek oka a kölcsönös elismerés elve, mely alapján az igazságügyi hatóságok nem értékeli egymás határozatait és nem folytatnak le külön vizsgálatot. Mint ahogyan azt a korábbi EUB gyakorlat is megmutatta, az Európai Unió jelenlegi kereti között az elv teljes megvalósulása irreális. Ugyanakkor a tagállamokok közötti különbségek értékelését az eljáró igazságügyi hatóságok kezébe helyezni indokolatlan visszalépés a kiadatási eljárás jogintézményébe. Következésképpen szükséges az európai elfogatóparancs alapvető jogok szerinti megtagadásának átgondolása és szükség esetén az „újabb" döntések revíziója. A Bíróság ismertetett ítélkezési gyakorlata alapján erre viszont csekély valószínűség mutatkozik.

VII. Záró gondolatok

Az európai elfogatóparancs több mint húsz éve váltotta fel az európai kiadatási eljárást. A kölcsönös elismerés elvére alapozva lehetővé tette, hogy büntetőeljárás lefolytatásának vagy szabadságvesztés-büntetés, illetve szabadságelvonással járó intézkedés végrehajtásának céljából egy gyors és gördülékeny eljárásban átadják az érintett személyt a kibocsátó igazságügyi hatóságnak.

A tagállamok a közös értékrendszer fennállása és a kölcsönös bizalom meglétére tekintettel, lemondtak a kiadatási eljárás garanciáiról, így harminckét bűncselekmény tekintetében áttörték a kettős inkrimináció elvét, lehetővé tették saját állampolgáraik átadását, leszűkítették a megtagadás lehetőségét, valamint megszüntették a miniszteriális szakaszt és a döntést teljes egészében igazságügyi hatóságok kezébe helyezték. Mindezek által az európai elfogatóparancs elérte legfőbb célkitűzését és a keresett személyek átadását átlagosan két hónapra rövidítette a kiadatásra jellemző egy másfél év helyett.

Jogintézménye ugyanakkor nem maradt problémáktól és kételyektől mentes. Az Európai Unió Bíróságának hozzá fűződő gyakorlata rámutat a tagállamok közötti gazdasági és politikai különbségek okozta ellentétekre. Az ismertetett döntések szerint folyamatos bővítésre került a végrehajtás megtagadásának lehetősége, így kérdéses, hogy valóban sikerült-e a kiadatás minden elemét hátra hagyni. Az EUB X.Y. ügyben hozott ítélete akarva-akaratlanul a kölcsönös elismerés elvének sérelméhez vezetett, ami így hátráltathatja az Unió büntetőügyekben folytatott igazságügyi együttműködését és visszalépést jelent a kiadatás intézményébe.[60]

Az európai elfogatóparancs rendhagyó történetében ugyanakkor kétségtelen az a tény, hogy létrehozása megerősítette a tagállamok közti szorosabb bűnügyi kooperációt, melynek eredményeképp többek közt megalkották a *büntetőügyekben kibocsátott európai nyomozási határozatról szóló* 2014/41/EU irányelvet, ami a tagállamok közötti bűnügyi együttműködés alapvető fontosságú jogintézménye. Az európai elfogatóparancs finomhangolása még nem fejeződött be. Az Európai Parlament és a Tanács 2024.

[60] Gellér 2024: i.m. 84-85. o.

november 27-én elfogadta a *büntetőeljárás átadásáról szóló 2024/3011 rendeletet*, melynek célja, hogy egyszerűbb legyen a büntetőeljárások átadása, valamint hogy a büntetőeljárás abban a tagállamban folytassák le, ahol az a leghatékonyabban lehetséges Az Európai Unió ehhez hasonló jogalkotási törekvései lehetőséget nyújthatnak egy egységes büntetőigazságügyi térség kialakítására, melyben kiemelkedő szerepet élvezhet az európai elfogatóparancs.

Kálmán Kinga:
Fluctuating Harmony – examining the relation between the Data Act and the GDPR

I. Introduction

Data management plays a key role in the European thinking about how to exploit the opportunities inherent in data-driven innovation. The growing volume of data is considered a key factor in more efficient decision-making concerning both the public and private sectors. Therefore, not only the collection of data, but also its sharing and reuse promises to contribute significantly to value creation for individuals and businesses, as well as for society in general.[1]

In reality, the collection, sharing and reuse of data may conflict with many interests that are protected under European Union and/or national legal frameworks, which results in the risk of infringement or other harm outweighing the expected value in the data in the eyes of many stakeholders. The result falls short in everyday data reuse and sharing practices.[2]

Having recognized this, the European Union has been active in this area, making significant efforts in recent years to exploit the underlying potential in data. The emerging new data law framework appears to break with the European Union's previous approach, which was fundamentally aimed at protecting information, especially personal data, along with a data minimisation approach, the central element of which is formed by the General Data Protection Regulation.[3]

In the first conceptual unit of this paper, I briefly outline the European Union's Data Act,[4] which, in contrast to other legislative acts affecting the data ecosystem, seeks to establish access to data and a data sharing ecosystem with a horizontal approach. The paper discusses in detail the main provisions of the Data Act relating to data access and sharing. Finally, I present the relationship and potential conflicts between the Data Act and the General Data Protection Regulation, which sheds light on the potential tensions between the two approaches from a broader perspective, as well as the problems of their joint application. I conclude the paper with summarizing the framework and the complex relationship system.

---

[1] Maximilian Grafenstein: Reconciling Conflicting Interests in Data through Data Governance. An Analytical Framework (and a Brief Discussion of the Data Governance Act Draft, the Data Act Draft, the AI Regulation Draft, as well as the GDPR). *HIIG Discussion Paper Series*, 2022. p. 8.
[2] Ibid. pp. 8-9.
[3] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC.
[4] Regulation (EU) 2023/2854 of the European Parliament and of the Council of 13 December 2023 on harmonised rules on fair access to and use of data and amending Regulation (EU) 2017/2394 and Directive (EU) 2020/1828.

II. Structure of the Data Act

The aim of the Data Act is to boost the European Union's data economy by liberating industrial data, optimising their accessibility and use,[5] with a fair distribution of the economic value derived from data among the actors of the data economy.[6]

The regulation is based on the recognition that during the use of certain connected products and related services, the data generated are attributable to at least two actors: on the one hand, to the manufacturer of the product and/or the provider of the related service, and on the other hand, to the person using it. However, the data generated most often remain with the manufacturer and the service provider, whilst users are generally not aware of the data they generate, or if they are aware, they do not have the opportunity to obtain such data.[7] Before presenting the data sharing framework, it is important to clarify the scope and basic concept of the Data Act.

II.1. Scope and basic concept of the Data Act

Within the meaning of the Data Act, "data" itself means any digital representation of acts, facts or information, and any compilation of such acts, facts or information, including in the form of sound, image or audiovisual recordings.[8] Data is a potential carrier of information, without reference to format, and is therefore adaptable to any data processing situation, although from the highlighted data categories (e.g. audiovisual recordings) the presumed predominance of digital data can be inferred.[9] This essentially means that any data generated during the use of a connected product or related service and designed to be retrievable may be subject to a data sharing obligation.

However, only raw and pre-processed data fall within the scope of the Data Act. By raw data, also known as source or primary data, the Data Act refers to automatically generated data points without any further data processing.[10] Pre-processed data are raw data that have been pre-processed to make them suitable for further processing and analysis, for example by cleaning or transforming. The data may have been collected by a single sensor or an interconnected group of sensors, for example in the case of devices used to measure temperature, pressure, flow rate, sound, pH value, liquid level, position, acceleration or speed.[11]
In contrast, information derived or deduced from such data, resulting from adding value or insights to the data, does not fall within the scope of the data sharing obligations under the Data Act. An example of this may be an autonomous vehicle that uses multiple sensors and mathematical models to create a 3D image of the environment in order to be

[5] Data Act: *Commission welcomes political agreement on rules for a fair and innovative data economy.* https://ec.europa.eu/commission/presscorner/detail/en/ip_23_3491 (Downloaded: 21 November 2025).
[6] European Commission: *Inception impact assessment of the Data Act.* https://openfuture.eu/wp-content/uploads/2022/03/Inception-impact-assessment.pdf (Downloaded: 21 November 2025).
[7] Recital (6) of the Data Act.
[8] Article 2 (1) of the Data Act.
[9] Kollár Gergő: Az adathasznosítás adatfogalmának meghatározási lehetőségei. *Közigazgatási és Infokommunikációs Jogi PhD Tanulmányok*, 2024/I., p. 16.
[10] Recital (15) of the Data Act.
[11] See: fn. 5. p. 3.

able to drive the vehicle independently, in which case the raw data from the sensors would fall within the scope of the data sharing obligation, whereas the 3D image would not.[12]

Moving on to the material scope of the law, connected product is defined by the Data Act as an item that obtains, generates or collects data relating to its use or environment, and which is able to communicate product data via an electronic communications service, physical connection, or device access, and whose primary function is not the storage, processing or transmission of data on behalf of any party other than the user.[13]

Therefore, products that primarily serve to store, process or transmit data (such as servers and routers) fall outside the scope of mandatory data sharing obligations, unless they are owned, rented or leased by the user. Similarly, the fact that a connected product (such as a wagon, aircraft or vehicle) uses certain infrastructure (such as railways, airports or motorways) to operate does not entitle the user of the connected product to access data generated by sensors forming part of the infrastructure. The user would only gain access if they had ownership or other contractual rights over the sensors built into the infrastructure.[14]

Accompanied related services include applications that could transmit commands to the connected product in order for the product to behave in a certain way. This could be, for example, an application to adjust the brightness of lighting or to control the temperature of a refrigerator, or an application downloaded alongside a smart washing machine that allows the environmental impact of the washing cycle to be measured based on data from various sensors in the machine and to adjust the cycle accordingly.[15] Related service therefore includes all data exchange between the connected product and the service provider that affects the operation of the connected product itself.

II.2. Data access and sharing framework introduced by the Data Act

The Data Act introduces a three-tier data sharing system. The first level is default, "by design" access, followed by access to be provided upon user requests in cases where the product and/or service cannot be designed to provide access to data by default. The third level is the data holder's obligation to make the data available to a third party at the user's request.[16] Data access and data sharing are based on a contractual relationship to be established mandatorily between the parties (data holder and user and/or third party).[17]

---

[12] Recital (15) of the Data Act.
[13] Article 2 (5) and Recital (14) of the Data Act.
[14] Library of the European Commission: *Commission publishes Frequently Asked Questions about the Data Act*. https://digital-strategy.ec.europa.eu/en/library/commission-publishes-frequently-asked-questions-about-data-act (Downloaded: 21 November 2025) p. 9.
[15] European Commission: *Data Act explained*. https://digital-strategy.ec.europa.eu/en/factpages/data-act-explained (Downloaded: 21 November 2025) p. 2.
[16] Tóth András*: A digitális átalakulás szabályozása az Európai Unióban*. Orac Kiadó, Budapest, 2024. pp. 110-112.
[17] Szilágyi Ferenc: Az adathozzáférést és az adatfelhasználást szabáIyozó szerződések és a szerződési jogi szabályok az EU Adatrendelet (Data Act) keretrendszerében I. rész, *Magyar Jog*, 2024/10., p. 580.

a) First level: Data sharing "by design”

Connected products and related services placed on the internal market of the European Union after 12 September 2026 must be designed, manufactured and/or provided with data sharing considerations in mind,[18] in such a way that product data, related service data and relevant metadata are easily, securely and freely accessible to users by default. The Data Act does not elaborate on this latter obligation in detail, only stipulating that connected products must be designed so that data are directly accessible from the data storage on the device or from a remote server.[19]

b) Second level: Access based on user requests

If users cannot directly access data from a connected product or related service, then upon the user's request, "readily accessible data" must be made available as soon as possible, together with the metadata necessary for interpreting and using such data.[20] Readily accessible data are product data and related service data that the data holder has lawfully obtained "without disproportionate effort beyond a simple operation". Access to data must be provided automatically upon the user's request, without examination or authorisation by the manufacturer or data holder. In cases where a connected product or related service is used by several individuals or organisations, the data holder must limit each user's access to the data generated by themselves, which possibility data holders are obliged to offer.[21]

c) Third level: Sharing data with third parties

Upon request by the user or a party acting on behalf of the user, the data holder must make readily accessible data and relevant metadata available to a third party in the format and manner described above for data access requests submitted by users. Such third parties may include, for example, repair shops where users take their out-of-warranty connected devices for repair, or providers of applications that offer functions beyond those offered by the related service.

Similar to data access requests from users, data holders may request a third party to continue to provide the necessary information within the framework of strictly necessary information to confirm that the person is an authorised third party. Whilst access to data for the user must be free of charge, data holders may charge remuneration if they make data available to third parties in business-to-business (B2B) relationships.[22]

III. The relationship between the Data Act and the General Data Protection Regulation

The Data Act and the General Data Protection Regulation are connected at numerous points. The Data Act generally states that it complements and does not prejudice the

[18] Article 3 (1) and 50 of the Data Act.
[19] Recital (22) of the Data Act.
[20] Article 4 (1) of the Data Act.
[21] Recital (21) of the Data Act.
[22] Article 5 (1) and Recital (46) of the Data Act.

General Data Protection Regulation and cannot be applied or interpreted in such a way as to narrow or limit the protection of personal data. [23] However, the application of the Data Act raises a number of comprehensive conceptual questions, or questions related to specific data processing institutions, which somewhat nuance this general statement. These include, inter alia, the determination of the personal data nature of data, the identification of participants in data access proceedings, the delimitation of the appropriate legal basis for data processing when accessing personal data based on the Data Act, and the conceptual positioning of data portability in the interaction of the two regulations.

III.1. Concept on personal data

A connected product, such as a smartwatch, a self-driving vehicle or even a connected refrigerator, may, among other data, generate data about an identified or identifiable natural person, i.e. a data subject within the meaning of the General Data Protection Regulation. In such cases, the question arises whether product data can also be considered personal data, and combined datasets may contain varying amounts of personal data. If other data and personal data are inextricably linked, the provisions and general principles of the General Data Protection Regulation, such as data minimisation, apply to the data, even if the dataset contains only a small amount of personal data. Aggregating data in a way that allows individual identification can transform non-personal data into personal data. These, even if they are not personal data at a given time, may become so in the future.[24] This may lead us to a situation where all data becomes personal data.[25]

The Data Act covers both personal and non-personal data, but in the case of personal data, imposing several restrictions and limitations on data access and sharing. It may be difficult for data holders to decide on a case-by-case basis whether they are dealing with personal data or not. In the event of incorrect classification, if data are considered non-personal data (when they were in fact personal data), there is a risk of violating the General Data Protection Regulation. On the other hand, however, data holders cannot play it safe and treat all product and related service data as personal data if they are not certain. Otherwise, they may also violate the data access rules of the Data Act. Therefore, although the Data Act does not expressly state that data holders have an obligation to prove whether data are personal data or not, as a result of the joint interpretation of the two pieces of legislation, it will be the task of data holders to carry out the (correct) classification.[26]

However, this classification is far from clear in the light of the current regulatory framework and case law, the starting point of which stems from different interpretative approaches to the concept on personal data. In the following, I briefly address these

[23] Recital (7) of the Data Act.
[24] Fondia: *Data Act and GDPR interplay*. https://fondia.com/en/en/insights/articles/data-act-and-gdpr-interplay (Downloaded: 21 November 2025).
[25] Nadezhda Purtova: The law of everything. Broad concept of personal data and future of EU data protection law. *Law, Innovation and Technology*, 10/1., p. 80.
[26] Freshfields: *When GDPR and Data Act clash: what Businesses need to know*. https://technologyquotient.freshfields.com/post/102j51u/when-gdpr-and-data-act-clash-what-businesses-need-to-know (Downloaded: 21 November 2025).

interpretative directions, highlighting the uncertainties that may have an impact on the application of the entire Data Act.

The interpretation of the concept on personal data is divided between absolute and relative approaches. According to the absolute approach to personal data, the personal nature of information does not depend on the identity of the data controller; the data's connection to the data subject is objective, so data processing occurs even if the data controller themselves cannot, but any other person is able to identify the data subject. Within this, certain perspectives distinguish according to whether a natural person can be identified using information stored or found at another data controller or elsewhere.[27] In contrast, according to the relative approach, what is important is whether the addressee, the data controller, and its subjective ability to link the given data to the data subject, i.e. whether the data qualifies as relating to the data subject based on their knowledge, information, and reasonable efforts. As a result, for example, whilst certain data may qualify as personal data for one person, they may not for others.[28]

Several cases have examined whether the data controller or a third party is able to identify data subjects either directly or indirectly. Case law is divided between absolute and relative interpretation, with constant evolution. Overall, a moderate orientation towards relative interpretation can be observed, but this does not appear to close the question. Below, I briefly summarise the essence of the most important decisions or guidelines issued concerning the two interpretative approaches.

a) Absolute approach to the concept on personal data

The Court of Justice of the European Union first interpreted the concept of personal data centrally in the 2016 Breyer case, in relation to the personal data nature of IP addresses. The decision stated: the fact that the additional data necessary to identify the user of a website are not held by the electronic media service provider, but by the internet access provider of this user, does not preclude dynamic IP addresses from constituting personal data.[29] However, the Court of Justice of the European Union pointed out that re-identification is primarily possible when it does not require a disproportionate amount of time, cost or effort, which restrictions point towards relative interpretation.[30]

In a later decision, the Court of Justice of the European Union also stated that in determining the identifiability of a natural person, "all means" must be taken into account "which are reasonably likely to be used" by the data controller "or another person" to identify the natural person "directly or indirectly". Therefore, for data to be classified as "personal data", it is not a requirement that all data enabling the identification of the person concerned be in the hands of one person".[31] Consequently, "indirect identification" of the data subject entails that supplementary information must be combined with other

[27] Czapári Dóra - Szőke Gergely László: Az adatvédelem és az adathasznosítás egyik kulcskérdése: a személyes adatok anonimizálása. *JURA*, 2022/4., p. 29.
[28] Schultz Márton: Az anonimizálás és az újraazonosítás aktuális kérdései, különös tekintettel a bírósági határozatok felismerhetetlenné tételére. *In Medias Res*. 2024/1., pp. 97-98.
[29] C-582/14. Breyer ECLI:EU:C: 2016:779 [54].
[30] C-582/14. Breyer ECLI:EU:C: 2016:779 [46].
[31] C-479/22. P. OC ECLI:EU:C: 2024:215 [48].

data for the purpose of identifying the data subject, which potentially originate from a person or source other than the data controller.[32] This approach has further been reiterated the Court of Justice of the European Union's decision in the IAB Europe case.[33]

Going beyond the above findings, the Court of Justice of the European Union decided that the vehicle identification number (VIN number) is not personal data in itself, but becomes personal data in relation to a person who reasonably has means that enable the data to be linked to a specific person. Therefore, the VIN number constitutes personal data of the natural person mentioned in the said certificate, provided that "the person who has access to the VIN number may have means that enable them to use it to identify the owner of the vehicle to which the VIN number relates, or to identify the person who may use the vehicle on a legal basis other than ownership". The Court of Justice of the European Union also stated that the VIN number as such does not constitute personal data for vehicle manufacturers if the vehicle to which the VIN number has been assigned is not owned by a natural person. However, it does not exclude that the VIN number may still constitute personal data even in these cases if this data is combined with other data. The Court of Justice of the European Union refers to case-by-case decision whether the addressees "becoming aware" of the VIN number may reasonably have means that enable them to link the VIN number to an identified or identifiable natural person, i.e. whether the VIN number constitutes personal data.[34]

In Hungary, the Data Protection Commissioner serving as the predecessor of the National Authority for Data Protection and Freedom of Information (NAIH), as well as the NAIH and the Supreme Court (Kúria), initially appeared to support the absolute interpretation. The Data Protection Commissioner stated that the personal data nature of certain data does not depend on there being only one way to access the given data.[35] In its opinion from 2012, the NAIH affirmed that "as long as the data controller has the possibility to link the data to an identified or identifiable natural person, the data constitute personal data, regardless of the circumstance that, as a result of some 'coding' procedure, the data cannot be linked to a specific natural person for the data processor."[36] In a 2022 decision, the Hungarian Supreme Court (Curia) evaluated as a method of indirect identification the case where the data subject can be identified even by comparing the anonymised data with information stored in authentic registers (in the case at hand, land registry data).[37]

b) Relative approach to the concept on personal data

In the most recent SRB case, the CJEU confirmed that pseudonymised data is not always personal data in all cases and for every person; if the risk of identification is insignificant, then the pseudonymisation may mean that the data is anonymous. The risk of identification must be "insignificant" if it is prohibited by law or impossible in practice, for example because it would involve a disproportionate effort in terms of time, cost and

[32] C-479/22. P. OC ECLI:EU:C: 2024:215 [51].
[33] C-604/22. IAB Europe ECLI:EU:C: 2024:214 [51].
[34] C-319/22. Scania ECLI:EU:C: 2023:837 [44]-[49].
[35] Data Protection Commissioner ABI 2004, 41.
[36] NAIH-2512/2012/V.
[37] Kúria 103.K.703.004/2022/16. [20] and [22].

labour. In the underlying case, the Court of Justice of the European Union rules that if pseudonymised data is transferred to a party that has no reasonable means to identify natural persons based on the pseudonymised data, the data shall not be considered as personal data for the receiving party.[38] In line with this, the European Data Protection Board has also taken the position that, as a general rule, data do not lose their personal data nature as a result of pseudonymisation.[39]

A similar decision was made by the Kúria in 2019, according to which, in the case of pseudonymised health data, coded data held by organisations without the decryption key do not constitute personal data and are not subject to data protection regulations.[40] Pseudonymisation is also accepted by the Article 29 Working Party (WP29) guidance, provided that any other data controller processing the same coded dataset would not be processing personal data, if the processing takes place in the separate system, re-identification is expressly excluded and appropriate technical measures have been taken in this regard.[41] Irreversible coding was also accepted by the NAIH in a decision as a form of anonymisation and stated that the availability of technology alone is not sufficient to identify data subjects.[42]

From the above, the only certain conclusion that can be drawn is that the personal data nature of data always depends on case-by-case assessment. However, the question arises as to how compatible the data access obligations and directions envisaged by the Data Act are with this assessment obligation. Are data holders obliged to ensure that users or third parties who do not qualify as data subjects are not able to identify the data subject by combining the transmitted data with other data using reasonable means? If so, to what extent is this possible in the case of mass data sharing? In my view, this dilemma is capable of hindering access to and sharing of data and pushing data holders towards a less proactive approach.

A possible resolution of the dilemma may be if the data holder collects, stores and/or shares as the least personal data possible concerning the data subject, to which end they design connected products and related services in such a way as to provide data subjects with the opportunity to use the devices anonymously or in the least intrusive manner possible, regardless of the legal basis on which they have the device. Data holders should also limit the amount of data leaving the device.[43]

---

[38] C-413/23 P. SRB EU:C: 2025:645.

[39] EDPB: *Guidelines 1/2025. on pseudonymisation*. https://www.edpb.europa.eu/system/files/2025-01/edpb_guidelines_202501_pseudonymisation_en.pdf (Downloaded: 21 November 2025).

[40] Kúria Pfv.20954/2018/6. [18].

[41] WP29: *Guidelines 4/2007. on the concept of personal data*. https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2007/wp136_hu.pdf (Downloaded: 21 November 2025) p. 22.

[42] NAIH/2020/1839/10.

[43] EDPB-EDPS: *Joint Opinion 2/2022 on the Proposal of the European Parliament and of the Council on harmonised rules on fair access to and use of data (Data Act).* https://www.edpb.europa.eu/system/files/2022-05/edpb-edps_joint_opinion_22022_on_data_act_proposal_en.pdf (Downloaded: 21 November 2025) p. 2.

In addition, data holders may be assisted by the anonymisation or pseudonymisation of personal data,[44] which could be achieved e.g., through the application of privacy enhancing technologies (PET). Anonymisation or pseudonymisation may be relevant, for example, when the data holder must respond to a user request where the requesting user is not the data subject, or when there are multiple data subjects who may all be users of the same connected product (e.g. a rented car). In such situations, the application of PETs can help ensure compliance with the General Data Protection Regulation.[45] Beyond pseudonymisation and anonymisation, the data holder is obliged to delete product and related service data - in accordance with the General Data Protection Regulation's principle of limited storage - after the expiry of reasonably defined retention periods.[46]

III.2. Identification of participants in data sharing

Identifying the actors involved in data sharing and delimiting their roles presents challenges when the General Data Protection Regulation and the Data Act must be applied simultaneously. The General Data Protection Regulation uses the concepts of "data controller" and "data processor", whilst the Data Act covers "data holders" and "users". When processing personal data, the data holder often also acts as a data controller. However, the roles may partially overlap. For example, a company that rents cars to natural persons may qualify as a user vis-à-vis the manufacturer, and as a data holder vis-à-vis the driver. In contrast, in the case of a natural person who is both a user and a data subject, when the company processes personal data - such as the car's location data - the company can be considered both a data controller and a data holder. It is important to understand that just because someone is in a certain role under the Data Act, they are not necessarily acting in the same capacity under the General Data Protection Regulation. For example, "user" does not always correspond to the concept of "data subject", and "data holder" does not always mean "data controller".

Although it is possible that data processors also participate in this setup, data processors as defined under the General Data Protection Regulation should not be considered to be acting as data holders. Nonetheless, data controllers may expressly authorise data processors to make data available to users.[47]

The roles in data sharing are therefore not predetermined and must be assessed on a case-by-case basis in accordance with the General Data Protection Regulation.[48] Clarity between overlaps or conflicts between roles may be a cardinal question, inter alia, when fulfilling user data access requests, when the user also qualifies as a data subject. It is not clarified whether, if a user who qualifies as a data subject approaches the data holder with an access request but does not specify the legal basis for their right of access (which they cannot be obliged to do), the request can be interpreted as an access request under both the Data Act and the General Data Protection Regulation, and if so, what obligations the

[44] At this point, it is worth noting that, due to the uncertain legal assessment of pseudonymization, complete anonymization is the safest technology for removing the personal nature of data.
[45] See: fn.14. p. 11.
[46] Recital (24) of the Data Act.
[47] Recital (22) of the Data Act.
[48] See: fn. 24.

data holder has if they do not qualify as a data controller under the General Data Protection Regulation: is the data holder obliged, for example, to make a decision on whether the request also qualifies as a request under the General Data Protection Regulation, or is it obliged to automatically involve the data controller in the settlement of the request? These questions remain to be answered for now.

III.3. Legal bases

The Data Act states in principle that the processing of personal data under the Data Act must have a valid legal basis under the General Data Protection Regulation, and that the Data Act alone does not constitute a legal basis for the data holder to collect or generate personal data.[49]

Data holders, users and third parties must therefore carry out the use of personal data based on a valid legal basis under the existing legal framework of the General Data Protection Regulation. Viable scenarios may involve where users of connected products only request access to their own personal data and authorise a third party to use such data; in this case, consent may be applicable as a legal basis provided the requirements set of Article 6(1)(a) of the General Data Protection Regulation are met.

However, the user of the product will not always be the same as the data subject. Instead, business users and third parties will be interested in data that either identify individuals on their own, or that can be linked to other data and then used to identify customers, employees or other persons - such as when a car rental service requests vehicle data from the manufacturer, or an airline requests flight data from aircraft manufacturers. In these cases, data access will only be achievable if one of the legal bases set out in Article 6 of the General Data Protection Regulation is applicable. The European Data Protection Board and the European Data Protection Supervisor remind that where consent is required under Article 5(3) of the ePrivacy Directive for the connected product as a terminal equipment, consent under Article 6 of the General Data Protection Regulation would be the most likely appropriate legal basis for the processing of personal data following the storage of or access to information already stored in the subscriber's or user's terminal equipment.[50] However, if the user is not the data subject, the Data Act alone cannot create a legal basis for providing access to personal data or making personal data available to a third party, so such actions cannot fall within the scope of data processing necessary for compliance with a legal obligation under Article 6(1)(c) of the General Data Protection Regulation.

If data subjects do not give consent and the data cannot be lawfully processed on another legal basis, data holders can easily find themselves in situations where they cannot fulfil a data access request under Article 4 of the Data Act without potentially violating the requirements of the General Data Protection Regulation.

A pragmatic way out of this dilemma would also be to oblige data holders, product users and third parties to use all available and economically reasonable means to anonymise

[49] Recital (7) of the Data Act.
[50] See: fn. 43. point 44.

datasets before sharing them, especially if the consent of data subjects cannot be obtained. Such anonymisation efforts should be encouraged not only for datasets that immediately enable the identification of individuals, but also for those that only enable identification after combination with other data in the possession of the product user or third party. Anonymising data requires that neither the data holder, e.g. the vehicle manufacturer, nor the product user under Article 4(1), e.g. the car rental company, should be able to identify individual data subjects. In this case, it must also be clarified who should bear the costs of anonymisation. If the parties cooperate and conclude agreements, they can negotiate the sharing of costs. If they do not reach an agreement and the data request is enforced by authorities or courts, the data holder may take into account the costs of anonymisation as part of applicable compensation.[51]

The relationship between the Data Act and the General Data Protection Regulation is not limited to the protection of users' and other data subjects' data, but Article 6 of the Data Act states that the receiving third party may only process the received personal data for the purposes and under the conditions agreed with the user, and is obliged to delete the data when they are no longer needed for the purpose under the agreement, without hindering the effective exercise of the right of access to data.[52] This framework incorporates the principles of lawful processing and limited storage into the structure of the Data Act, following the logic of the General Data Protection Regulation.[53]

III.4. Data portability

The Data Act fundamentally complements the right to data portability guaranteed to data subjects by the General Data Protection Regulation in four main respects:

a) *opening data portability to legal persons;*
b) *covering non-personal data and personal data processed on any legal basis whilst the General Data Protection Regulation only allows data portability in the context of data processing based on consent or contract;*
c) *introducing immediate accessibility by default,*[54] *and*
d) extending its scope to both actively provided and passively observed data.

However, the Data Act creates confusion by presenting data portability in a different light. Firstly, data portability as such is not articulated in the legal text. Instead, there is the user's right of access and the user's right to share data with third parties, whilst the term data portability remains in the recitals. In contrast, the right of access under the General Data Protection Regulation is more akin to transparency requirements under the

[51] Axel Metzger - Heike Schweitzer: *Shaping Markets: A Critical Evaluation of the Draft Data Act*. https://ssrn.com/abstract=4222376 (Downloaded: 21 November 2025) pp. 28-29.
[52] Recital (23) of the Data Act.
[53] Bárbara da Rosa Lazarotto*:* The Right to Data Portability: A Holistic Analysis of GDPR, DMA and the Data Act. *European Journal of Law and Technology*. 15/1., 2024.
[54] Tommaso Crepax, Mitisha Gaur, Barbara da Rosa Lazarotto: *Measuring data access and re-use in the European Legal Framework for Data, from the General Data Protection Regulation (GDPR) law to the Proposed Data Act: the case of vehicle data*. https://open-research-europe.ec.europa.eu/articles/3-192 (Downloaded: 21 November 2025) p. 22.

Data Act, which the Data Act rules complement.[55] The two data subject rights, as well as the user rights under the Data Act, must be clearly distinguished from each other.[56]

According to some perspectives, it can be inferred from the Data Act's provisions on data portability that the data holder will not necessarily be obliged to transfer a copy of the data to a third party. Instead, one possible interpretation of the Data Act is that these data are accessible through the manufacturer's or cloud service provider's server, via on-site access to the data. However, requiring on-site access to data would dramatically change the right to data portability in the Data Act, as it would degrade it to a simple "right of data access", and the data would remain under the control of data holders, who could unilaterally decide whether the data are accessible only through on-site access or through data portability. According to another perspective - with which I also agree - the argument for in-situ access becomes even more fragile in the light of recital (35) of the Data Act and its express reference to the Data Act's complementary nature to the right provided in Article 20 of the General Data Protection Regulation. Thus, although it would be expedient to choose the wording more clearly, a holistic interpretation of the law allows the conclusion that data portability is not limited to in situ access.[57]

Article 12(5) of the General Data Protection Regulation states that measures taken to fulfil data subjects' requests, including the right to data portability, must be carried out free of charge. It is not clear whether this provision can be interpreted as excluding remuneration for making data available. Since the General Data Protection Regulation's right to data portability also allows direct data transmission between data controllers, where technically feasible, it is not clear whether the General Data Protection Regulation can be interpreted as excluding compensation under Article 9 of the Data Act for the original data controller in the case of such direct data transmissions. Article 12(5) of the General Data Protection Regulation does not prescribe any fee for data subjects (except where requests are manifestly unfounded or excessive) but does not expressly exclude the possibility that original data controllers may charge receiving data controllers a fee for data portability requests. Recital (35) of the Data Act further increases uncertainty by stating that the data subject cannot in any way be prevented from exercising their rights under the General Data Protection Regulation - including the right to data portability - by seeking redress in accordance with that Regulation, if the data holder and the third party cannot agree on the conditions for access to data. It would therefore be worth clarifying how the General Data Protection Regulation's - seemingly - free requests for data portability relate to data access requiring compensation in the Data Act.[58]

Although there are clear overlaps between the General Data Protection Regulation and the Data Act, it remains doubtful how effectively they will work in the practical implementation of the right to data portability. It may be necessary to determine under

[55] Recital (24) of the Data Act.
[56] Mahsouli Farid: *A Data Act to reconcile stakeholders' tensions arising from Data portability? Critical analysis of the Commission's proposal from a consumer's point of view*. https://arno.uvt.nl/show.cgi?fid=171034 (Downloaded: 21 November 2025) p. 22.
[57] See fn. 53.
[58] Inge Graef - Martin Husovec: *Seven Things to Improve in the Data Act*. https://ssrn.com/abstract=4051793 (Downloaded: 21 November 2025).

which regulation the data subject or user is requesting the right to data portability, especially if the basis of the request is personal data processed on the basis of consent or contract, since the right to data portability can be exercised under both the General Data Protection Regulation and the Data Act. However, this will only become apparent when the two regulations are applied simultaneously in each case. In addition, the uncertainties arising from the interpretation of the concept of personal data, as well as from the different data processing roles – as outlined in the preceding sections - may also arise here.

By establishing a multi-level right to data portability, individuals could potentially gain greater control over their personal and non-personal data in a cross-sectoral environment. However, since the three regulations have different scopes and concepts, it remains unclear how individuals will be able to exercise the right to data portability effectively, in a manner beneficial to them and to the market. It is therefore essential that the interpretation of the multi-layered right to data portability does not create confusion and does not hinder individuals' rights, instead of providing them with more opportunities. Although the Data Act contains a clause declaring the primacy of the General Data Protection Regulation, the overlap between thee different pieces of legislation may cause uncertainties. Conflicts are expected to be resolved on a case-by-case basis, through the joint interpretation of the two regulations.[59]

IV. Conclusion

In this paper, I presented the European Union's legislative efforts towards a data ecosystem based on open access to data. Since the Data Act is the only one of the three pieces of legislation to cover data sharing horizontally it was elaborated in greater detail. Following a review of the legislative framework, I examined the relationship of the Data Act to the General Data Protection Regulation.

The central dilemma of examining the relationship system is the interpretative uncertainty of the concept of personal data, which is divided along two main trends in case law: according to the absolute approach, data are objectively personal in nature, regardless of the identity and capabilities of the data controller, whilst the relative interpretation is based on the reasonable possibilities of the data controller in assessing identifiability.

In the world of connected products, this uncertainty is particularly problematic, as data generated by smartwatches, self-driving vehicles and other IoT devices often mix personal and non-personal elements, making it difficult for data holders to decide whether, in providing access, they must simultaneously comply with the complex requirements of the General Data Protection Regulation. The situation is further complicated by the fact that the two regulations use different terminology: whilst the Data Act uses the concepts of "data holder" and "user", the General Data Protection Regulation uses the categories of "data controller" and "data processor", which roles often show overlaps or vary depending on context.

[59] See fn. 53.

Regarding legal bases, it is particularly problematic that the Data Act does not in itself create a legal basis under the General Data Protection Regulation for the processing of personal data, yet it prescribes data access obligations, resulting in a dilemma when data subjects do not consent to data processing, but the access obligation still exists. In the area of data portability, there may also be significant overlaps and unclear questions, particularly regarding the relationship between compensation and free provision, and regarding choosing the suitable provisions under which users may exercise their rights.

As a conclusion of my analysis, the objectives and provisions of Community legislation promoting open data access and sharing may conflict with the fundamentally privacy-friendly, data minimisation approach of the General Data Protection Regulation. According to my conclusions, these legal interpretation and application difficulties cause significant legal uncertainty for data holders, who risk violating both pieces of legislation simultaneously, which may ultimately hinder data sharing and the development of the digital economy. To solve the problem, I have considered the consistent application of the principle of data minimisation, the use of privacy enhancing technologies and the development of anonymisation techniques, whilst emphasizing that fundamentally a legislative simplification would be needed to resolve the overlaps and contradictions between the two regulations. Ultimately, I point out that although, according to the legislator's intention, the Data Act and the GDPR complement each other, in practical application such a significant gap yawns between normative expectations and feasibility that is difficult to bridge without the development of uniform case law and further legislative clarifications.

Páll Imre Borisz:
A közigazgatási típusú adatvédelmi eljárások kialakulása és helye a hazai jogrendszerben

I. Bevezetés

Aki a Magyar Tudományos Akadémia Doktori Tanácsa által jegyzett tudományági nómenklatúra[1] alapján próbálja az adatvédelmi jogot elhelyezni, a humán- és társadalomtudományok körében a IX. osztályig (Gazdaság- és jogtudományok) és azon belül az Állam- és jogtudományok (09 01 00) besorolásig akadálytalanul eljuthat, azonban a meglehetősen szerteágazó jogterület további tipizálása már közel sem ennyire egyértelmű.

Amennyiben a személyes adatok védelme körében kizárólagosan a közigazgatási (hatósági) eljárások vizsgálata áll a tudományos érdeklődés fókuszában,[2] úgy még mindig azzal szembesül a kutató, hogy az Európai Alapjogi Charta által nevesített alapvető jog védelmét az EU általános adatvédelmi rendeletének (GDPR)[3] szabályai és végső soron az Európai Unió Bíróságának (EUB) az esetjoga alapozza meg, így az Európai jog (09 01 24) tudományági prioritással bír.

Ha viszont jogforrási irányból közelítünk, és a hazai adatvédelmi jog hatályos forrásait próbáljuk feltérképezni, akkor a nemzetközi jogi dokumentumoktól az európai uniós jogforrásokon át az Alaptörvényig, az Ákr.-ig és – a *„globális összehasonlításban is egyedi”*[4] intézményrendszert megtestesítő – Infotv.-ig, továbbá számos ágazati jogszabályig jutunk, tehát egy meglehetősen komplex jogforrási rendszer tárul elénk.

További vizsgálati szempont lehet az egyes jogágak adatvédelmi rendelkezéseinek, illetve ilyen tartalmú eljárásainak összevetése vagy ezen eljárások egymástól való éles elhatárolása. Erre vonatkozó példaként említhető egyes nevesített személyiségi jogok védelme, vagy messzebbről közelítve a magánszféravédelem, a jegyző által lefolytatott birtokvédelmi eljárás magánterület kamerás megfigyelése körében, vagy az ún. „ombudsmani típusú” adatvédelmi vizsgálat és az adatvédelmi hatósági eljárás.

A fenti szempontokon túl bemutatható a hazai adatvédelmi jog elméleti és jogtörténeti aspektusból is, ugyanis az a magánjogi magánszféravédelemtől a nemzetközi jogi

---

[1] MTA: *Tudományági nómenklatúra*. https://mta.hu/doktori-tanacs/tudomanyagi-nomenklatura-106809 (Letöltve: 2026.03.03.).

[2] De még ebben az esetben is két kutatási irány adódik: 1) Közigazgatási jog, közigazgatás-tudomány (09 01 05), valamint 2) Közigazgatási eljárásjog (09 01 06).

[3] Az Európai Parlament és a Tanács (EU) 2016/679 RENDELETE (2016. április 27.) a természetes személyeknek a személyes adatok kezelése tekintetében történő védelméről és az ilyen adatok szabad áramlásáról, valamint a 95/46/EK rendelet hatályon kívül helyezéséről (általános adatvédelmi rendelet)

[4] Sziklay Júlia: *Visszaemlékezés a kezdetekre - az alapjogvédő ombudsman*. In: Péterfalvi Attila (szerk.): Szemelvények az információs jogok felügyeletének elmúlt 25 évéből. Budapest, 2020, 5. o. https://naih.hu/files/NAIH-jubileumi-szemelvenyek-az-informacios-jogok.pdf (Letöltve: 2026.03.03.)

privacy-védelmen és az alkotmányjogi megközelítésű információs önrendelkezési jogon át a ma hatályos, GDPR által megvalósuló önálló alapvető jogként védendő, uniós jogi megközelítés mint folyamat és fejlődési ív is tárgyalható.

Jelen tanulmány a személyes adatok közigazgatási típusú védelmének kialakulását mint folyamatot célozza bemutatni és az adatvédelmi jog fejlődési fázisainak és irányzatainak megfelelő új tipológiát nyújtani, eközben megpróbál egyensúlyozni az elméleti és a gyakorlati szempontok között, nem veszítve szem elől ugyanakkor a közigazgatási eljárásjogi fókuszt sem.

II. A személyes adatok közigazgatási típusú védelmének kialakulása

A személyes adatok védelme az amerikai *privacy* irodalomban gyökerezik, amelyet Warren és Brandeis 1890-es cikke alapozott meg. A *privacy*, illetve a *right to privacy* e konstrukcióját jelen tanulmányban a magyar nyelven azt Szabó Endre Győző „A személyes adatok védelméhez és a közérdekű adatok megismeréséhez fűződő jog" c. írása[5] alapulvételével összefoglaló Téglásiné Kovács Júlia által bemutatott értelemben használom.[6]

Az európai kontinensen a XX. század első felében elsősorban a magánszféravédelem körében tárgyalta a szakirodalom a személyes életkörülmények védelmét, beleértve a képmás és más személyes adatként azonosítható információk védelmét is. Ekkor azonban még nem önállósult az adatvédelmi jog. Magyarországon e tárgyban a korszak legkiemelkedőbb tudományos művét Balás P. Elemér írta 1941-ben, melyben a személyiségi jogokról értekezik.[7] Balás e korszakban a bírósági joggyakorlat fontosságát hangsúlyozta: *„azért is főforrása a bírói gyakorlat a személyiségi jogi megismerésnek, mert még hiányzik az az évezredes tapasztalat, mely a magánjog egyéb ágai mögött áll."*[8]

A II. világháború tapasztalatai felértékelték ugyan a magánszféra védelmét, de egészen az 1960-as évek végéig, immáron egy másik új technológia, a számítógépes adatfeldolgozás megjelenéséig kellett várni az adataink védelmét érintő magasabb szintű szabályozásra. E

[5] Szabó Endre Győző: A személyes adatok védelméhez és a közérdekű adatok megismeréséhez fűződő jog. In: Schanda Balázs – Balogh Zsolt: *Alkotmányjog – Alapjogok*. Pázmány Press, Budapest, 2019.

[6] *„Az angolszász jogfejlődés során a fényképezőgépek megjelenésekor Warren és Brandeis a Harvard Law Review folyóiratban 1890-ben megjelent Right to privacy című cikkükben a privacy fogalmát az egyedülléthez (háborítatlansághoz) való jog szükségszerű vívmányaként fogalmazták meg. A szerzők szerint a privacy védelméhez fűződő jog nem szerződésből vagy konkrét jogviszonyból fakadó bizalmon alapul, hanem az egész világgal szemben fogalmazódik meg. Kifejtik, hogy privacy már korán túllépett az egyén pusztán fizikai értelemben vett védelmén. A különbség a gondolatok és érzések irodalmi vagy művészeti megfogalmazásban tett szándékos és nyilvános kifejezése, valamint ezeknek a hétköznapi életben, sokszor nem szándékos, nem a széles közvéleménynek szánt megnyilvánulásai között van. A jognak szavatolnia kell, hogy azok a tények, amelyekkel a nyilvánosságnak nincsen dolga, védelemben részesüljenek."* Téglásiné Kovács Júlia: A személyes adatok védelméhez fűződő jog. In: Bódi Stefánia – Schweitzer Gábor (szerk.): *Alapjogok*. Ludovika Egyetemi Kiadó, Budapest, 2021, 175. o.

[7] Balás P. Elemér: Személyiségi jog. In: Szladits Károly (szerk.): *Magyar Magánjog. Első kötet*. Grill, Budapest 1941, 635-674. o.

[8] Uo. 637-638. o.

korszak első adatvédelmi jogszabályai sokfélék voltak, ugyanis nemzeti szinten hozták őket. Közös bennük, hogy elsősorban a nagy állami adatbázisok átláthatóságát célozták biztosítani.[9]

A világ első, kifejezetten adatvédelmi tárgyú törvényét Németország (NSZK) Hessen tartományában fogadták el 1970-ben, melyet Svédország 1973-ban, az NSZK 1977-ben, Franciaország pedig 1978-ban követett,[10] míg az Egyesült Királyság az Európa Tanács 1981. évi 108. sz. Egyezménye nyomán 1984-ben fogadta el első adatvédelmi törvényét.[11]

Mindeközben az egykori szovjet blokk országaiban hivatalosan nem jöhetett szóba az amerikai gyökerű privacy-alapú tudományos gondolkodás, ahogyan a két világháború közti magyar magánjog hagyományait is kerülte az akkori pártállami ideológia. Gömbös Ervin 1984-ben megjelent „Informatika és hatalom" című könyvének előszavában a KSH elnöke pártállami öntudattól eltelve fejtette ki a szocialista adatvédelem további fejlesztésének szükségtelenségét: *„a tőkés társadalmakban az egyén bizalmatlan az elektronikus adatgyűjtéssel és -feldolgozással szemben […]. Az adatok megfelelő kezelését, a személyi jogok védelmét jogrendszerünk biztosítja."*[12] Bár 1977-ben az akkor hatályos Ptk. 83. § (1) bekezdése már valóban kimondta, hogy a gépi adatfeldolgozás *„nem sértheti a személyhez fűződő jogokat"*, ennek mind tartalmi, mind nyelvtani tarthatatlanságát a szakirodalomban Könyves Tóth Pál kimutatta.[13]

Vámos Tibor már az 1982-ben publikált, egyébként egy informatikai törvény szükségességét hangsúlyozó cikkében megjegyezte, hogy *„az egyénnek a saját személyes szférára való jogaira az angolban régóta köznapian használt privacy szóra magyar szavunk sincsen"*.[14]

A magyar adatvédelmi jog szempontjából azonban Sólyom László 1983-as, a személyiségi jogok elméletéről szóló könyve, majd pedig a jogállami fordulatot követően az Alkotmánybíróság korai döntései jelentik az érdemi kezdetet.

III. A közigazgatási típusú adatvédelem jelenlegi intézményrendszerének előzményei

Az 1989-1990. évi közjogi rendszerváltást jogállami forradalomként interpretáló elmélet szerint az információszabadság körében történt szemléletváltás lényege, hogy a „pártállam

[9] Jóri András: *Adatvédelmi kézikönyv*. Osiris, Budapest, 2005, 24. o.
[10] Péterfalvi Attila (szerk.): *Adatvédelem és információszabadság a mindennapokban*. HVG-ORAC, Budapest, 2012, 25. o.
[11] Peter Carey: *Data Protection. A Practical Guide to UK and EU Law*. Oxford University Press, Oxford, UK, 2009, 3. o.
[12] Nyitrai Ferencné: Előszó. In: Gömbös Ervin: *Informatika és hatalom*. Statisztikai Kiadó Vállalat, Budapest, 1984, 10. o.
[13] Könyves Tóth Pál: Adatvédelem és információszabadság. *Világosság*, 1990/8–9., 622. o.
[14] Vámos Tibor: Információ és társadalom. *Magyar Tudomány*, 1982/11., 802. o.

információs filozófiáját kellett ellenkezőjére változtatni: *átláthatatlan állam - átlátható állampolgár vs. átlátható állam - átláthatatlan állampolgár*."[15]

Ennek egyik alkotmányos következménye az adatvédelmi biztos intézményének a létrehozása lett, ugyanakkor az 1990-es években kialakított, a korábbi magyar alkotmányjogi hagyományok által nem ismert ombudsmani intézményt az Alaptörvény nyomán a 2012. január 1-jétől hatályba lépett Infotv. a Nemzeti Adatvédelmi és Információszabadság Hatósággal (NAIH) váltotta fel.

Az átalakítás miatt kötelezettségszegési eljárás indult Magyarországgal szemben. Az ügy az Európai Unió Bírósága elé került, ahol az EUB nagytanácsának 2014. április 8-i ítélete szerint Magyarország azáltal sértette meg az általános adatvédelmi rendeletet (GDPR) megelőzően hatályban volt 95/46/EK irányelvet (adatvédelmi irányelv), hogy az adatvédelmi biztos hatéves mandátumának lejárta előtt szüntette meg ezt a tisztséget.[16] Azt azonban érdemes megemlíteni, hogy e döntés a hazai adatvédelem szintjének csökkenését nem állapította meg.

2018. május 25. napja lényeges mérföldkő – más megfogalmazás szerint *„történelmi jelentőségű pillanat"*[17] – a hazai, de egyébként az uniós adatvédelmi jog számára is. Ettől kezdve ugyanis kötelező erejűek és közvetlenül alkalmazandóak a GDPR által rögzített adatvédelmi minimumkövetelmények. A GDPR 51. cikkének (1) bekezdése írja elő, hogy a *„rendelet alkalmazásának ellenőrzéséért egy vagy több független közhatalmi szerv (felügyeleti hatóság) felel"*. Ezt az előírást 2018. július 26. napjától, az Infotv. 38. § (2a) bekezdése hatálybaléptetése útján teljesítette a jogalkotó, amikor a NAIH-ot nevezte meg kijelölt hatóságként.

A GDPR szakított az addigi *privacy*-alapú adatvédelmi jogi megközelítéssel, amelynek a *common law*-ból eredő gyökerei visszanyúlnak Warren és Brandeis klasszikusnak nevezhető cikkéig.[18] A 95/46/EK irányelv 1. cikkének (1) bekezdése még kifejezetten „a magánélet tiszteletben tartásához való jogukat a személyes adatok feldolgozása tekintetében" szófordulatot tartalmazta, egyúttal a *privacy* fogalmát a magánélettel azonosítva. A GDPR azonban már nem hivatkozik a *privacy* fogalmára, amit eleve nem sikerült jól átültetni a magyar tudományos szóhasználatba.

Sólyom László a *„right of privacy, vagyis az általános személyiségi jog"* definíciót alkalmazta.[19] A szakirodalom ismeri azt a véleményt is, amely szerint a magánszféra

[15] Majtényi László: *Az információs szabadságok.* CompLex, Budapest, 2006, 17. o.
[16] C-288/12. Európai Bizottság kontra Magyarország ECLI:EU:C:2014:237.
[17] Boros Anita: Az autonóm államigazgatási szervek, a kormányhivatalok és az önálló szabályozó szervek nem hatósági eljárásai. In: Boros Anita – Patyi András (szerk.): *A hazai közigazgatási (nem hatósági) eljárások alapvető jellemzői a hatékonyság tükrében*. Dialóg Campus, Budapest, 2020, 259. o.
[18] Samuel D. Warren – Louis D. Brandeis: The Right to Privacy. *Harvard Law Review*, 1890/5., 193-220. o.
[19] Sólyom László: *A személyiségi jogok elmélete*. Közgazdasági és Jogi Könyvkiadó, Budapest, 1983, 218. o.

védelme, valamint a Warren és Brandeis által kifejtett *right to privacy* koncepciója fogalmilag nem azonos.[20]

A legújabb, már nem *privacy*-alapú szakirodalom a személyes adatok védelmét – alkotmányjogi megközelítésben – továbbra is mint információs önrendelkezési jogot értelmezi: *„Az Alkotmánybíróság tehát az Alaptörvény alapján is a személyes adatok védelméhez való jogot nem hagyományos védelmi jogként értelmezi, hanem annak aktív oldalát is figyelembe véve, információs önrendelkezési jogként. A személyes adatok védelméhez való jognak eszerint az a tartalma, hogy mindenki maga rendelkezik személyes adatainak feltárásáról és felhasználásáról."*[21]

IV. A magánszféravédelemtől az adatvédelemig terjedő jogi koncepciók egy lehetséges tipológiája

Warren és Brandeis 1890-es cikkétől a Szladits Károly által szerkesztett Magyar Magánjogban Balás P. Elemér által 1941-ben jegyzett, a magánszféra védelméről szóló fejezeten át Sólyom László 1983-as „A személyiségi jogok elmélete" című munkájáig, pláne a GDPR 2018-as bevezetéséig hosszú út vezetett. Azt is láthatjuk, hogy bár voltak a magyar magánjognak olyan elemei, amelyeket a hazai adatvédelmi jogi gondolkodás korai előzményeinek tekinthetünk, azonban azt is tudomásul kell vennünk, hogy a ma hatályos adatvédelmi jogi rezsim elméleti előzményei és alapjai számos külföldi elemet is tartalmaznak. Ezek előrebocsátásával az alábbiakban az egyes elméleti megközelítések fogalmi elhatárolását kísérlem meg, korántsem állítva, hogy más megnevezések és meghatározások ne bírnának létjogosultsággal.

IV.1. A privacy-alapú megközelítés

A személyes adatok védelméhez fűződő jog mint alapvető jog a nemzetközi jogfejlődés viszonylag kései terméke, az 1970-es évek végétől beszélhetünk róla, Magyarországon pedig leginkább a jogállami fordulat óta. Az adatvédelmi jogi normák első generációja az államok általi, gépi úton történő adatfeldolgozást szabályozta.

Két forrásból eredt az adatvédelmi szabályok elméleti igazolása. Egyrészt az amerikai privacy irodalom (1890) és annak a II. világháborút követő nemzetközi térhódítása szolgált az adatvédelmi normák első generációjának elméleti megalapozásául, másrészt az általános személyiségi jog és az információs önrendelkezéshez való jog (legalábbis a Magyarországon Sólyom László által ekként interpretált) német alkotmányelméleti konstrukciója járult hozzá az önálló adatvédelmi jog kialakulásához. Ebből következően szükségszerűen beszélhetünk egy *privacy*-alapú, amerikai, a *common law* világában gyökerező, valamint egy nem *privacy*-alapú, kontinentális, alapvetően német alkotmányjogi megközelítésről.

[20] Szabó Máté Dániel: Kísérlet a privacy fogalmának meghatározására a magyar jogrendszer fogalmaival. *Információs Társadalom*, 2005/2., 44–54. o.
[21] Sulyok Tamás – Villám Krisztián – Deli Gergely: A személyes adatok védelme az Alkotmánybíróság gyakorlatában. In: Szabó Endre Győző (szerk.): *Az Infotörvénytől a GDPR-ig*. Ludovika Egyetemi Kiadó, Budapest, 2021, 46. o.

Egy további, sajátos európai színfolt az olasz jogtudós, Stefano Rodotà szellemi hagyatéka. Az alapvetően *privacy*-alapú, de egyben emberi jogi, és különösen is az emberi méltóságot alapul vevő adatvédelmi jogi megközelítés[22] az EU első adatvédelmi biztosa (Rodotà) hivatali idejét követően honfitársa és utódja, Giovanni Buttarelli útján továbbra is áthatotta az európai adatvédelmi jogi gondolkodást.[23] Ezt a *privacy*-megközelítésű adatvédelmi gondolkodást fejti ki Buttarellinek a nagy technológiai óriásokkal szemben állást foglaló posztumusz megjelent kiáltványa.[24]

Az amerikai és az olasz *privacy*-alapú megközelítés közötti különbség abban rejlik, hogy az amerikai jogi gondolkodásban teljesen természetes a bírói út igénybevétele, enélkül a *common law* létre sem jöhetett volna. Ezzel szemben az európai *privacy*-védelem állami szabályozást feltételez, amelynek terjedelméig az adatalanyok aztán közigazgatási hatósághoz, a vagyonosabbak pedig jogi képviselőjük útján közvetlenül bírósághoz fordulhatnak többek között személyes adataik védelme érdekében.

IV.2. A privacy-szerű megközelítés

A hazai adatvédelem megkerülhetetlen úttörője a magánjogász Sólyom László, az Alkotmánybíróság (AB) első elnöke, akinek az 1970-es évek végétől kifejtett tudományos munkássága nyomán jöttek létre azok a magánjogi elméleti alapok, amelyekre az 1990. évi közjogi rendszerváltást követően épülhetett az adatvédelmi jog közjogi intézményrendszere és alkotmánybírósági gyakorlata. Sólyom tudományos munkásságát e vonatkozásban mindösszesen egyetlen, szemantikai jellegű kritikai észrevétel érte, mely szerint az Alkotmánybíróság Sólyom téves értelmezése következtében az általános személyiségi jogot az emberi méltóság egyik megfogalmazásának tekinti.[25] Ugyanakkor Koltay ennek jelentőséget nem vizsgált tárgyunk, a közigazgatási típusú adatvédelmi eljárások, hanem kifejezetten az általános személyiségi jog magánjogi azonosítása körében tulajdonít.[26]

Ebből a magánjogi gyökerű tudományos megközelítésből fakad Szabó Máté Dániel azon felismerése, hogy a magánszféra védelme, valamint Warren és Brandeis *privacy*-koncepciója fogalmilag nem azonos. Definíciója szerint a *privacy „az egyén joga ahhoz, hogy magáról döntsön”*, vagyis az önrendelkezéshez való jog intézményével azonosítja azt: *„mindenki maga döntheti el, mi lesz a saját sorsa, mit tesz magával, a testével és a rá*

---

[22] Lásd pl.: Stefano Rodotà: *Privacy, libertà, dignità*. *Discorso conclusivo della Conferenza internazionale sulla protezione dei dati.* 26th International Conference on Privacy and Personal Data Protection., Wrocław, 2004. https://www.garanteprivacy.it/home/docweb/-/docweb-display/docweb/1049293 (Letöltve: 2026.03.03.).

[23] Rocco Panetta: Afterword. Privacy 2030: To give humans a chance. In: Giovanni Buttarelli: *Privacy 2030: A New Vision for Europe*. https://assets.contentstack.io/v3/assets/bltd4dd5b2d705252bc/bltb34ecc8261028db4/privacy_2030_vision_for_europe.pdf (Letöltve: 2026.03.03.).

[24] Buttarelli: i.m. 5. o.

[25] Pokol Béla*:* Gondolatok az alkotmánybírósági döntések elvi alapjaihoz. *Jogelméleti Szemle*, 2012/1. https://ojs.elte.hu/jesz/issue/view/532/317 (Letöltve: 2026.03.03.)

[26] Koltay András: Az „általános személyiségi jog” azonosítása felé. In: Koltay András – Török Bernát (szerk.): *Sajtószabadság és médiajog a 21. század elején 4*. Wolters Kluwer, Budapest, 2017, 271. o.

vonatkozó ismeretekkel."[27] Jóri András is felismerte a *privacy* fogalmához képest szűkebb jelentést, mégis – jobb híján – magánszféraként tárgyalta azt.[28]

Álláspontom szerint ugyanakkor itt indokolt lehet a „*privacy-szerű adatvédelem*" fogalmának használata. Ez egyrészt nem zárja ki a személyes adatok védelmének az önrendelkezéshez való jog körében történő tudományos értelmezését, másrészt kifejezi, hogy nem a hazai szerves jogfejlődés eredményéről van szó, hanem külföldi, illetve esetünkben nemzetközi jogi behatásról, harmadrészt pedig arra is alkalmas, hogy kibővítve a magánszféra-védelem fogalmát, egyszerre fogja át a Ptk. 2:43. § e) pontja szerinti, személyiségi jogi perben bírói útra tartozó magánjogi aspektust, valamint az Európai Unió általános adatvédelmi rendelete (GDPR) szerinti közigazgatási (77. cikk (1) bek.), valamint közvetlen bírósági (79. cikk (1) bek.) típusú adatvédelmet.

Bármely típusú adatvédelmi jogi eszköz igénybevételéről legyen ugyanis szó, végső soron – hasonlóan a *common law* jogrendszerekhez – bírói útra fog tartozni a jogvita végleges rendezése, beleértve a Kúria jogerős döntése elleni alkotmányjogi panasz AB általi elbírálását, szükség esetén a határozat megsemmisítését és az elsőfokú bíróság elé való visszautalását is.

A fenti, *privacy*-alapú megközelítést tovább részletezte Majtényi László, aki tudományosan ismertette azt a nem szükségszerű magyar sajátosságot, hogy adatvédelem és információszabadság nem csak törvényileg került egységes szabályozásra, de ennek elméleti alapja is van: *„A személyes adatok védelme és az információszabadság […] különös viszonyban állnak egymással, mely viszonyt az egyensúly, ellentét, kölcsönös feltételezettség, egymás általi meghatározottság, egymás kiegészítése jellemez."*[29]

A *privacy*-szerű adatvédelmi megközelítés kapcsán fontos hangsúlyozni, hogy a GDPR-t megelőző elméleti konstrukcióról van szó. Természetesen önrendelkezésről kizárólag a GDPR 6. cikk (1) bek. a) pontja szerinti jogalap esetén lehet ma már csak értekezni. Az állami és az üzleti érdekeltségek ugyanis kikényszerítették a személyes adatok 6. cikk (1) bek. b)-f) pontjai szerinti jogalapokkal történő jogszerű kezelésének elismerését, amelyekre az adatalany („érintett") önrendelkezésének joga ráhatással nem bír. Az érintett hozzájárulása egyenértékű bármely jogalappal, leszámítva, hogy talán annyiban még gyengébb is, amennyiben a legbizonytalanabb jogalapnak számít, hiszen a megadott hozzájárulás bármikor indokolás nélkül visszavonható. Ezért az adatkezelők sokszor inkább olyan jogalapot választanak, ami megkerüli az érintett saját személyes adatai feletti önrendelkezési jogának hatékony érvényesíthetőségét (pl. „jogos érdek").

IV.3. A *data protection* alapú megközelítés – egy európai uniós kísérlet

Bár az Európai Unió általános adatvédelmi rendelete nem tartalmazza a *privacy* kifejezést, amiből arra lehetne következtetni, hogy az EU a privacy-védelemtől teljesen függetlenített adatvédelmi jogi rezsimet hozott létre, ezt maga az európai adatvédelmi

[27] Szabó: i.m. 44–54. o.
[28] Jóri: i.m. 11. o.
[29] Majtényi: i.m. 24. o.

ombudsman árnyalta egy GDPR-kommentár előszavában.[30] Ugyanezen kommentár, mintha csak az európai jogértelmezés széttagoltságát szándékolta volna alátámasztani, a GDPR 25. cikke szerinti *beépített és alapértelmezett adatvédelem („data protection by design and by default")* elvéről szóló fejezetében megállapítja, hogy a GDPR 25. cikkének nincs a korábbi adatvédelmi irányelv szerinti megfelelője.[31] Ugyanakkor a 25. cikk szerinti elvről folyó viták *privacy by design* elnevezés alatt folynak,[32] a kanadai Ontario tartomány volt adatvédelmi biztosának, Ann Cavoukiannak a nemzetközi privacy-védő közösségre nagy hatást gyakorló kifejezése nyomán.[33]

Miközben tehát az európai jogtudósok között sincs konszenzus a *data protection* és a *privacy protection* pontos fogalmáról, azok tartalmáról és az általuk pontosan lefedett jogterületről, még a GDPR által – a *privacy* fogalmának teljes mellőzése és az adatvédelem (*data protection*) hangsúlyozása által félreérthetetlenül – egyértelművé tett, a globális *privacy*-védelemből önállósodó európai uniós megközelítés sem tekinthető általánosan elfogadott nézetnek. Buttarelli például úgy tudta, hogy nem az amerikai, illetve nemzetközi jogból fejlődött ki az európai adatvédelmi jog, hanem fordítva, a világ mintegy felében jelenlévő szabályozásokat az európai megközelítés erősen befolyásolta.[34]

A fentiekre tekintettel nem állapítható meg, hogy általánosan elfogadott lenne az európai tudományos életben az adatvédelem (*data protection*) mint önálló jogi szakkifejezés és jogintézmény használata. Jelenleg sokkal inkább a globálisan elfogadott *privacy*-védelem körében tárgyalják az Európai Unió kötelező jogi aktusa (GDPR) által adatvédelemnek (*data protection*) nevezett terület elméleti hátterét. Ezt indokolhatja az is, hogy a GDPR elfogadásához egy kompromisszumokkal és mintegy négyezer szövegmódosítással terhelt út vezetett, ami miatt a GDPR inkább tekinthető egy politikai alku- és lobbifolyamat eredményének, semmint egy letisztult jogelméleti háttérrel rendelkező jogi aktusnak.

IV.4. A *data privacy* alapú megközelítés

Az előző pontban hivatkozott Buttarelli-szöveg is tartalmazza a *data privacy* kifejezést[35], ami a *common law* országok jogirodalomában létező megközelítés, ugyanakkor független a GDPR-ban használt, bizonytalan elméleti hátterű *data protection* szóhasználattól. Az itt *data privacy alapúnak* nevezett megközelítés legalaposabb kifejtése Robert C. Posthoz

[30] Giovanni Buttarelli: Foreword. In: Christopher Kuner – Lee A. Bygrave – Christopher Docksey (szerk.): *The EU General Data Protection Regulation (GDPR) – A Commentary*. Oxford University Press, Oxford, 2020. v. o.
[31] Lee A. Bygrave: Article 25. Data protection by design and by default. In: Christopher Kuner – Lee A. Bygrave – Christopher Docksey: i.m. 573. o.
[32] Uo.
[33] Ann Cavoukian: *Privacy by Design.* https://www.ipc.on.ca/en/media/1826/download?attachment (Letöltve: 2026.03.03.)
[34] Giovanni Buttarelli: The EU GDPR as a clarion call for a new global digital gold standard. *International Data Privacy Law*, 2016/2., 77. o. https://doi.org/10.1093/idpl/ipw006
[35] Buttarelli az alábbi forrásra hivatkozott: Graham Greenleaf: Global Data Privacy Laws 2015: 109 countries, with European Laws Now a Minority. (2015)133 Privacy Laws & Business International Report, February 2015.

köthető.[36] Post az Európai Unió Bírósága által tárgyalt Google Spain ügy tanulságait elemezte. Az írás betekintést enged az amerikai, *privacy*-szemléletű gondolkodásba, amelyen keresztül értelmezi a döntést és annak jogi hátterét, valamint a döntés következményeit. Az Európai Unióban elsősorban az internetes keresőmotorokból történő törlés, azaz az elfeledtetéshez való jog (*right to be forgotten*) érvényesítése szempontjából volt mérföldkő az ítélet, Post azonban a szólásszabadság amerikai doktrínája szempontjából, vagyis a demokratikus nyilvánosság felől közelítve tárgyalja a témát.

A szerző számára ellentmondásos ítélet két lényegi szempontot elemez: a már nem hatályos 95/46/EK irányelv által biztosított, elfeledtetéshez való jog által érintett *privacy*-t és a kifejezés szabadságát. Post szerint a döntés mindkettőt rosszul elemzi. A szerző, hangsúlyozottan még a GDPR előtti európai uniós adatvédelmi jogra utalva, a közösségi jogban létező *privacy* két altípusát határozza meg, amelyek több, az EU-n kívüli állam jogában is megtalálhatóak: *adatalapú privacy* (*data privacy*; amelyet az adatvédelmi irányelvből vezet le, azt a világ legfontosabb adatvédelmi szövegének nevezve: *„probably the most influential data privacy text in the world”*[37]) és a társadalmi nyilvánosság szempontjából releváns, *méltóság alapú privacy* (*dignitary privacy*; amelyet az Európai Unió Alapjogi Chartájának 7. cikkéből vezet le: *„Article 7 of the Charter protects what we may call «dignitary privacy».”*[38]). Az *adatalapú privacy*-t tehát Post az adatvédelmi irányelv rendelkezéseiből vezeti le, mint információs önrendelkezési jogot. A *méltóság alapú privacy*-t viszont már az Európai Unió Alapjogi Chartájának 7. cikkéből eredezteti.

Post elméleti konstrukciója a GDPR által meghatározott keretek között is jól használható, világosan elkülöníti a *privacy* funkcióit, vagyis azt, hogy a *privacy* általa meghatározott két típusa mely jogi tárgy védelmét szolgálják, amely által maga a *privacy* általános fogalma is jól elkülönül a magánszféravédelemtől önállósult adatvédelmi jogtól mint alapvető jogtól, függetlenül attól, hogy egyes uniós jogi normák mind a *privacy*, mind a személyes adatok védelme szempontjából relevánsak lehetnek.

IV.5. A privacy fiduciárius modellje

A magyar adatvédelmi jog elmélete és közigazgatási modellje szempontjából inkább csak érdekességként említhető Jack M. Balkin megközelítése.[39]

A szerző megállapítása szerint egyes vállalatok működését nemcsak az információs aszimmetria és az átláthatóság hiánya jellemzi, hanem tudatosan dolgoznak ki olyan üzleti modelleket, beleértve termékeiket és szolgáltatásaikat is, amelyek a legkülönfélébb módszerekkel gyűjtik személyes adatainkat, miközben a felhasználók csak megbízni

[36] Robert C. Post: Data privacy and dignitary privacy: Google Spain, the right to be forgotten, and the construction of the public sphere. *Duke Law Journal*, 2018/5., 980-1072. o. https://scholarship.law.duke.edu/cgi/viewcontent.cgi?article=3928&context=dlj (Letöltve: 2026.03.03.)
[37] Uo. 984. o.
[38] Uo. 991. o.
[39] Jack M. Balkin: The fiduciary model of privacy. *Harvard Law Review*, Vol. 2020/134, 11-33. o. https://harvardlawreview.org/wp-content/uploads/2020/10/134-Harv.-L.-Rev.-F.-11.pdf (Letöltve: 2026.03.03.)

tudnak a szolgáltatóban, mert azok a működésükről és ügyfeleik személyes adatainak kezeléséről a lehető legkevesebb információt teszik könnyen hozzáférhetővé, vagy egyenesen eltitkolják azokat.

Az új technológiák elterjedése, például a dolgok internetje (*internet of things*) által, egyrészt azt eredményezi, hogy a digitális eszközök egyre hatékonyabban szolgálják használójukat, másrészt azonban azt is, hogy ezen eszközök egyre több információt gyűjtenek, sokszor azon kereskedelmi célból, hogy használatuk függőséget okozzon. Ráadásul ezen eszközök a használóik környezetében tartózkodókról, akár azok tudta nélkül is gyűjtenek személyes adatokat, lehetővé téve ezzel további befolyás gyakorlását.

Ezért Balkin azt vizsgálja, hogy értelmezhető-e *bizalmi kapcsolatként* (*fiduciary relationship*) az ilyen, IKT-szektorhoz kötődő szolgáltatás igénybevétele. Ezt Balkin digitális *„information fiduciary”*-ként fogalmazza meg, amelyet itt *„információs fiducia”*-ként fordítok. Az *„információs fiduciák”* három kötelezettséget foglalnak magukba a szolgáltató („fiduciárius”) részéről a végfelhasználó irányában: a bizalmasság, a gondosság, valamint a lojalitás kötelezettségét.

Ez a koncepció egyedi, alternatív megoldási javaslatot eredményez személyes adataink védelmére, amely első olvasatra nem illeszkedik a ma hatályos GDPR rendelkezései által alkotott uniós adatvédelmi jogi rezsimbe.

Ugyanakkor az amerikai Első Alkotmánykiegészítés, valamint az 1996. évi Telecommunications Act 230. szakasza által nyújtott kivételi szabályok összehasonlító elemzését lehetővé teszi Balkin tanulmánya, ugyanis a GDPR 85. cikke *(„a személyes adatok kezelése és a véleménynyilvánítás szabadságához és a tájékozódáshoz való jog”*) hasonló kivételi kört hivatott meghatározni a társadalmi nyilvánosság biztosítása érdekében.

V. A személyes adatok közigazgatási típusú védelme mint rendszer – eljárások és eljáró szervek

Amikor a személyes adatok közigazgatási hatósági úton történő védelmét tekintjük át, a gyakorlatban is tapasztalhatjuk a fentiekben bemutatott elméleti konstrukcióknak megfelelő eljárásjogi sokféleséget. E részben tehát már adottnak vehetjük mind a polgári jogtól, mind pedig a bírói hatalmi ágtól történő elkülönülést. Sőt, alkotmányjogi megközelítésben már nem az információs önrendelkezéshez való jogként, hanem az Európai Unió Alapjogi Chartájának 8. cikk (1) bekezdése szerinti, önállósult alapvető jogként tekinthetünk a személyes adatok védelmére még akkor is, ha a Charta II. címe a „Szabadságok”, nem pedig az alapvető jogok terminológiát alkalmazza.

Maga a GDPR a (4) preambulumbekezdésében már kifejezetten önálló alapvető jogként interpretálja a személyes adatok védelméhez fűződő jogot, azaz itt már nem a *privacy*-védelem keretében jelenik meg a védendő jogi tárgy: *„nem abszolút jog, azt az arányosság elvével összhangban, a társadalomban betöltött szerepének függvényében kell*

figyelembe venni, egyensúlyban más alapvető jogokkal". E megfogalmazás talán megnyugtatóan reflektál a szakirodalomban korábban pejoratív értelemben felvetődött „adatvédelmi fetisizmus"[40] kritikájára.

Emellett azonban a magánszféravédelem és a személyiségi jogok védelme körében továbbra is nyitva maradt a bírói út, valamint igénybe vehető az Alkotmánybíróság előtt az alkotmányjogi panasz mint általános alapjogvédelmi eszköz is, ugyanakkor megszűnt az adatvédelmi biztos intézménye. Így tehát egy viszonylag új és sajátos, a polgári jogi és alkotmányjogi jogvédelmet kiegészítő, közigazgatási típusú (alap)jogvédelmi rezsim jött létre a közelmúltban.

V.1. A közigazgatási típusú adatvédelem köre

Az első hazai adatvédelmi törvény (Avtv.) nyomán létrehozott adatvédelmi biztos intézménye a hatalmi ágak megosztása kontextusában független jogállású, alkotmányvédő szerv volt, amely ellensúlyt képezett a törvényhozó és a végrehajtó hatalmi ág között.[41] E megközelítés értelmében tehát az 1995-től 2011-ig létezett adatvédelmi biztos intézménye mindhárom klasszikus hatalmi ágon kívül helyezkedett el, az Alkotmánybírósággal egy szinten, szemben a 2012-től működő, autonóm államigazgatási szervként létrehozott NAIH-hal.[42]

Somody úgy érvel, hogy az ombudsmani intézmény hatósági jogkörrel történő felruházása *„kifejezetten ellentétben áll az ombudsman-intézmény lényegével"*, ezért kizártnak tartható az ilyen irányú jogalkotás.[43] Csakhogy az Európai Unió nem tudományos megközelítések, hanem a gyakorlati tapasztalatok alapján várta el már az adatvédelmi irányelv alapján is a tagállami adatvédelmi hatóságok létrehozását. Mivel tagállami implementáció volt szükséges, egyes tagállamok megőrizték a már meglévő adatvédelmi biztos intézményét, és közigazgatási hatósági hatáskörökkel ruházták fel azokat.

Ehhez képest sem a GDPR-t megelőző magyar jogalkotás, sem maga a 2018. május 25. napjától kötelezően alkalmazandó GDPR nem hozott újdonságot az adatvédelem intézményének közigazgatási hatósági jellegűvé válásában. Mivel az Infotv. megőrizte a korábbi adatvédelmi biztos vizsgálati eljárását, legalábbis annak elnevezését, ez ún. ombudsmani típusú adatvédelmi eljárássá alakult, ami az Infotv. ma hatályos 52. § (2) bekezdése értelmében nem minősül közigazgatási hatósági eljárásnak.

Arról lehet érdemi vitát folytatni, hogy ha egy autonóm államigazgatási szerv hoz egy elvileg nem kötelező erejű döntést, amellyel szemben nem létezik bírói jogorvoslat, úgy az valóban ombudsmani jellegű-e, vagy csak nevében maradt az. Mivel a NAIH vizsgálati eljárásának egyik lehetséges következménye, hogy hivatalból indított hatósági

[40] Nagy Marianna: *Interdiszciplináris mozaikok a közigazgatási jogi felelősség dogmatikájához*. ELTE Eötvös Kiadó, Budapest, 2010. 130. o.
[41] Bán-Forgács Nóra: *A rendszerváltás és az adatvédelmi ombudsman Magyarországon*. L'Harmattan, Budapest, 2022, 19. o.
[42] Bán-Forgács Nóra: *Az adatvédelmi ombudsman intézménye Magyarországon*. L'Harmattan, Budapest, 2021, 59-60. o.
[43] Somody Bernadette: *Az ombudsman típusú jogvédelem*. ELTE Eötvös Kiadó, Budapest, 2010, 86. o.

eljárássá fordul át, amennyiben például a vizsgált adatkezelő nem hajtja végre a vizsgálati eljárásban neki címzett intézkedést, úgy ez tulajdonképpen az adatvédelmi hatósági eljárásnak egy *de facto* előkészítő szakaszaként is felfogható.

Bár bírósági esetjog egyelőre nem áll rendelkezésre, így csak elméleti felvetés marad, de az általános közigazgatási rendtartás (Ákr.) 7. § (2) bekezdése szerinti definíció alapján hatósági ügy mindaz az intézkedés, amely során *„a hatóság döntésével az ügyfél jogát vagy kötelezettségét megállapítja, jogvitáját eldönti, jogsértését megállapítja”*, így amennyiben az ombudsmani típusúnak nevezett adatvédelmi vizsgálat ilyen intézkedést tartalmaz, úgy felvethető, hogy az ilyen eljárás is az Ákr. tárgyi hatálya alá eső, bírói törvényességi kontroll alá rendelhető eljárástípus. De önmagában annak ténye, hogy a klasszikus hatalmi ágakon kívülre elhelyezett adatvédelmi biztosi intézményt egy autonóm államigazgatási szerv váltotta fel, indokolja, hogy a vizsgálatot is a közigazgatási típusú adatvédelmi eszközök közé soroljuk, függetlenül az ilyen döntések jogerejétől és bírói felülvizsgálatától, vagy annak hiányától.

Ehhez képest az Infotv. 32. címe szerinti adatvédelmi hatósági eljárás kétséget kizáróan közigazgatási jogi jogvédelmi eszköz, amelyet már a GDPR alkalmazását megelőzően is indíthatott hivatalból a NAIH, érintett állampolgári kezdeményezésre azonban csak 2018. május 25-étől nyílik lehetőség az EU tagállamaiban, így Magyarországon is, amennyiben a kifejezetten *rá vonatkozó* személyes adat jogsértő kezelését feltételezi az érintett. Ez utóbbi, érintetti kérelemre induló eljárás az Európai Unió Alapjogi Chartájának, valamint a GDPR-nak a rendelkezésein alapul, amelyeket a hazai adatvédelmi jogban az Infotv., valamint az Ákr. eljárásjogi rendelkezései egészítenek ki.

V.2. A személyes adatok védelmének eljárásjogi rendszere

Számos esetben nehezen vagy egyáltalán nem határolhatóak el bizonyos eljárások az adatvédelem kérdésétől. Kétségtelenül a bírósági útra tartozó személyiségi jogi jogvédelem körébe esik a Ptk. 2:43. § e) pontjának megsértése, azaz a magántitokhoz és a személyes adatok védelméhez való jog megsértése miatt indított jogvita rendezése, vagy például a birtoklás – polgári jogi – tényét érintő, jegyzői birtokvédelmi eljárás ún. „szomszéd kamerás” ügyekben, ahol a kifogás tárgya rendszerint a más magántulajdonára irányuló kamerás megfigyelés, illetve akár a kamera felszerelésének puszta ténye.

Annak egyértelmű elhatárolásához, hogy mi esik az adatvédelem és mi pl. a személyiség- vagy birtokvédelem körébe, érdemesnek tűnik az elméleti előzmények ismertetése után immár gyakorlati alapon is egy rövid kitekintést tenni. Még egy empirikus tapasztalatokon nyugvó elemzés sem lehet azonban teljeskörű, hiszen sokszor maga az ügyfél sem tárja az eljáró közigazgatási hatóság elé (és vagy kiderül a becsatolt iratokból, vagy nem is sejti az ügyintéző), hogy eljárásával párhuzamosan bírósági eljárás is folyik, aminek esetleg egy „leágazása” a hatósági adatvédelmi eljárás. Sőt, számos esetben eleve az adatalany jogi képviselője javasolja ügyfelének a hatósági eljárás kezdeményezését azt célozva, hogy a hatóság szerezze be azokat a hitelt érdemlő bizonyítékokat, amelyeket ő aztán ügyfele érdekében más – nem adatvédelmi jogi – ügyben bíróságon fel tud használni (kártérítés, vagyonmegosztás, rágalmazás stb.).

Ha rendszerként próbáljuk interpretálni a személyes adatok védelmét, annak intézményi hátterét, akkor főszabály szerint a bírósági és a közigazgatási utat szükséges figyelembe vennünk. A ma Magyarországon igénybe vehető közigazgatási, valamint bírói út intézményi háttere az alábbiak szerint rendszerezhető vázlatosan.

a) Közigazgatási típusú adatvédelem (egyfokú eljárás)

- ombudsmani típusú vizsgálat (Infotv. 51/A. § - 58. §; nem minősül közigazgatási hatósági eljárásnak)
- hatósági eljárás (GDPR 77. cikk (1) bek., Infotv. 60. § - 61/D. §, Ákr.)

Nem minősül közigazgatási hatósági eljárásnak a jegyző birtokvédelmi eljárása, pontosabban van olyan nézet, ami szerint csak a végrehajtási szakaszban, az Ákr. és a Vht. szabályainak alkalmazása során válik azzá.[44] Fontos azonban megjegyezni, hogy a kamerás megfigyelésekkel kapcsolatos birtoksértés tárgyában indult birtokvédelmi eljárás esetében sem jogkérdést vizsgál a jegyző a Ptk.-n, valamint a 17/2015. (II. 16.) Korm. rendeleten alapuló eljárásában, hanem a zavarás tényének meglétét, avagy annak hiányát.[45]

Az Ákr. alapján az eljáró hatóság szemlét rendelhet el a tényállás tisztázása céljából.[46] Azonban nem minősül az adatvédelmi hatóság által lefolytatott szemlének, amikor a jegyzőt keresi meg ilyen szemle lefolytatása végett, és annak eredményét használja fel a tényállás tisztázása keretében. Ugyanakkor a jegyző nem folytat adatvédelmi hatósági eljárást, csupán eleget tesz az őt megkereső hatóság felhívásának, ezzel mégis államigazgatási hatósági jogkört gyakorolva.

b) Bírósági úton történő adatvédelem

- GDPR 79. cikk (1) bek.-én alapuló adatvédelmi per
- Infotv.-en alapuló adatvédelmi kifogás: a bírósági adatkezelési műveletek ellenőrzése (Infotv. 71/A-C. §)
- jogorvoslat hatósági döntéssel szemben (közigazgatási per: GDPR 78. cikk (1) bek. alapján)

A közigazgatási határozatok törvényességének bírósági ellenőrző funkcióját ugyanakkor közel sem a GDPR vezette be, hanem általánosságban már az 1989-es alkotmánymódosítás megteremtette annak lehetőségét,[47] tehát azt hazai alkotmányos vívmánynak tekinthetjük.

[44] Gaál János – Kajó Cecília: *Birtokvédelmi kézikönyv*. ORAC Kiadó, Budapest, 2023, 262. o.
[45] Uo. i.m. 166. o.
[46] Ivancsics Imre – Fábián András: *Hatósági jogalkalmazás a közigazgatásban*. Dialóg Campus, Budapest, 2020, 105-106. o.
[47] Patyi András – Varga Zs. András: A közigazgatási eljárásjog alapjai és alapelvei. In: Patyi András – Varga Zs. András (szerk.): *A magyar közigazgatás és közigazgatási jog általános tanai. V. kötet.* Dialóg Campus, Budapest, 2019, 43. o.

A GDPR 79. cikkén alapuló perben az általános illetékességi szabályok érvényesülnek, míg a 78. cikken alapuló közigazgatási perben – a NAIH mint alperes székhelyére is tekintettel – minden esetben a Fővárosi Törvényszék jár el elsőfokon, a Kúria pedig másodfokon. A bírósági eljárást egészítheti ki az előzetes döntéshozatali eljárás (EUMSZ 267. cikk b) pont alapján), amennyiben az eljáró bíróság uniós jogot érintő autentikus jogértelmezést kér az Európai Unió Bíróságától az eljárást érintő jogi aktus kapcsán.

Nem minősül a személyes adatok bírósági védelme eszközének, de tartalmilag lehet adatvédelmi jellege is a személyiségi jogi jogvédelemnek (Ptk. 2:43. §), a polgári jogi birtokvédelemnek (Ptk. 5:7. §), vagy a büntetőjogi „jogvédelemnek" (Btk. 219. §, 422. §-422/A. §) is.

A hazai alkotmányjog a klasszikus értelemben vett bírói hatalmi ágon kívül, önálló jogi fórumként ismeri az Alkotmánybíróságot (AB). Szintén nem minősül az adatvédelem hagyományos jogi eszközének az alkotmányjogi panasz (Abtv. 26. § (1), Abtv. 26. § (2), Abtv. 27. § (1) bek.) intézménye, de egyes AB határozatok fontos forrásai az adatvédelmi jog alkotmányos értelmezésének, mint például a személyi szám alkotmányellenességét kimondó 15/1991. (IV. 13.) AB határozat, vagy az újabb gyakorlatból a NAIH uniós jogból fakadó hatáskörét érintő és a személyes adatok védelméhez fűződő jogot ismételten védelmi típusú alapjogként interpretáló 3110/2022. (III. 23.) AB határozat.

Végezetül megemlíthető még a strasbourg-i emberi jogi bíróság (EJEB), amely előtt az Európa Tanács 1981. évi, 108. sz. Egyezményének megsértése esetén – a nemzetközi bírói fórum befogadhatósági kritériumainak teljesülése, főszabály szerint pedig a hazai összes bírósági jogorvoslati lehetőség kimerítése esetén – szintén eljárás kérhető.

VI. Összegzés

Az elemzés mind elméleti, mind eljárásjogi oldalról áttekintette a közigazgatási típusú személyes adatvédelem közjogi kontextusát.

Előbbi tekintetében a tanulmány a hazai adatvédelmi jogi szakirodalomban új tipológiát vázolt fel az adatvédelmet mint folyamatot átfogó elméleti irányzatok időbeli és földrajzi megjelenését követve. Ezáltal remélhetőleg vázlatosan áttekinthetővé vált a *privacy*-védelem, a magánszféravédelem és az adatvédelem magyarországi kialakulásának elméleti háttere és az egymáshoz kapcsolódó nemzetközi, regionális, valamint hazai fejlődési íve és tudományos háttere.

Az eljárásjogi oldalt pedig mint rendszert ismertette az elemzés az intézményrendszeren és eljárásokon keresztül, külön bemutatva a közigazgatási hatósági aspektust is, az ombudsmani típusú vizsgálattal összevetve. Ennek következtében megállapítható, hogy a magyar adatvédelmi jog által nyújtott eljárásjogi lehetőségek európai színvonalúak, azonban a GDPR rendelkezései minden tagállamban azonos szintű, egységes végrehajtásának megvalósíthatósága továbbra is nyitott kérdés marad.

Abstracts

Krisztián Édes: Regression or evolution? – The relationship between the European Arrest Warrant and the institution of extradition

The European Arrest Warrant has replaced the previously lengthy extradition procedures since 1 January 2004. With its adoption, an efficient and simple surrender procedure came into force, which is able to respond to the changed nature of crime. However, today, both the Member States and the Court of Justice of the European Union continuously challenge the legal institution of the European Arrest Warrant and in some aspects it goes back to the old extradition. In light of this, it is appropriate to map the current relationship between surrender and extradition and to describe the practice of the European Arrest Warrant. In my study, I analyze the relationship between the two legal institutions using a descriptive and critical method, as a result of which I conclude that it is necessary to rethink the current framework of the European Arrest Warrant, since for its survival it is necessary to create harmony between the protection of fundamental rights and efficiency. The study highlights that if this further development does not take place, then in addition to the European Arrest Warrant, the principle of mutual recognition based on mutual trust will also be at risk.

Keywords: extradition procedure, european arrest warrant, mutual recognition, fundamental rights, european judicial cooperation in criminal matters, Court of Justice of the European Union

Kálmán Kinga: Fluctuating Harmony – examining the relation between the Data Act and the GDPR

The paper examines the European Union's Data Act, which seeks to establish a horizontal data access and sharing ecosystem, marking a departure from the EU's previous data minimisation approach centred on the General Data Protection Regulation (GDPR). The analysis explores the relationship and potential conflicts between the Data Act and the GDPR, highlighting tensions between the two regulatory approaches and challenges in their joint application. The Data Act aims to boost the EU's data economy by liberating industrial data and optimising their accessibility and use, introducing a three-tier data sharing system comprising default "by design" access, access upon user request, and data holder obligations to make data available to third parties at the user's request. However, the application of the Data Act raises numerous comprehensive conceptual questions related to specific data processing institutions. The central dilemma is the interpretative uncertainty of the concept of personal data, which is divided along two main trends in case law: the absolute approach, where data are objectively personal in nature regardless of the data controller's identity, and the relative interpretation based on the reasonable possibilities of the data controller in assessing identifiability. Additional challenges include legal basis dilemmas, as the Data Act does not itself create a legal basis under the GDPR for processing personal data, and data portability complications regarding

compensation and free provision. These legal interpretation and application difficulties cause significant legal uncertainty for data holders, potentially hindering data sharing and digital economy development.

Keywords: Data Act, personal data, access, sharing, legal basis, data subject, user

Páll Imre Borisz: The development and place of data protection procedures of public administration in the Hungarian legal system

The European Union's General Data Protection Regulation (GDPR) was enacted by the EU legislators as a result of the consensus of the Member States. However, the uniform application of the normative provisions of the new data protection legal regime that relies on the different enforcement rules of the Member States, has not been organically integrated into the traditions of domestic data protection, either theoretically or practically. Accordingly, the analysis identifies the milestones of the development of administrative-type personal data protection in Hungary from two perspectives. On the one hand, it presents the legal trends and academic approaches that have influenced the development of domestic data protection, thus interpreting the appearance of individual theories as a process. As a result, the study introduces a new typology starting from the concept of the "right to privacy", from which "data protection" as a fundamental right emerged in a century. On the other hand, it presents administrative data protection as a system. This approach provides an overview of the different types of procedures and the bodies involved, distinguishing between judicial, administrative, ombudsman-type and Constitutional Court procedures related to the protection of personal data.

Keywords: data protection, General Data Protection Regulation (GDPR), Hungary, public administration, right to privacy