KÖZIGAZGATÁSI ADATVÉDELEM AZ ADATGAZDASÁG, A MESTERSÉGES INTELLIGENCIA ÉS A PLATFORMDEMOKRÁCIA KORÁBAN

Páll Imre Borisz*

„Remota itaque iustitia quid sunt regna,
nisi magna latrocinia?”
(Szent Ágoston: *De Civitate Dei*)

1. Bevezetés

A fenntartható fejlődési célok közül a *béke, igazság és erős intézmények* témaköre régóta foglalkoztatja az európai gondolkodókat, így jelen tanulmányban való felvetése és aktualitása remélhetőleg nem szorul külön indokolásra és igazolásra.

Egy modern tömegtársadalomnak a fennálló jogrendbe, és annak – legalább eljárásjogi értelemben vett – igazságos voltába vetett bizalma jogállami keretek és piacgazdasági viszonyok kontextusában nagymértékben függ attól, hogy az állam polgárai milyen szintű jogvédelemben részesülhetnek jogaik vélt vagy valós sérelme esetén.

Napjainkban különösen igaz ez a különböző online platformok útján megvalósuló személyes adatkezelések tekintetében, függetlenül attól, hogy állami vagy magánszektorba tartozó adatkezelőről van-e szó, hiszen a digitalizáció megkerülhetetlen megatrenddé vált az elmúlt évtizedekben, sokszor egyébként kihívás elé állítva a jogalkalmazót, hogy a szólás szabadsága, vagy a személyes adatok védelme minősüljön-e erősebb alapjognak.

* A Nemzeti Közszolgálati Egyetem Közigazgatás-tudományi Doktori Iskolájának doktorandusza.

E tanulmány fókusza két, első megközelítésben talán egymással össze nem függőnek tűnő aspektusra irányul: egyrészt az uniós adatvédelmi jog globális – geopolitikai – kontextusba helyezésére, másrészt a hazai, közigazgatási típusú adatvédelmi hatósági eljárásoknak a közigazgatási szankciók végrehajtása vonatkozásában az EUB ítélkezési gyakorlatára.

Mindez a hazai közigazgatás befolyásának közel sem a saját hiányosságainak betudható, regionális és globális korlátaira vonatkozó következtetések levonására ad lehetőséget.

1. Az adatvédelmi fetisizmustól a nagy sakktábláig – kontextusba helyezhető-e a GDPR?

A közigazgatási jogi felelősség egyes jogdogmatikai kérdéseinek nagyívű elemzése közben Nagy Marianna kevéssé hízelgő megjegyzést tett a hazai adatvédelem intézményrendszerére és az azt kialakító és működtető jogászságra, az írás 2010. évi megjelenésére tekintettel alighanem az akkor még hatályos Avtv.-re és az azt 2012. január 1-jétől hatályon kívül helyező Infotv. tervezett szabályozási koncepciójára utalva:

> „[…] az adatvédelmi szabályozás indokoltságához a 21. században nem férhet kétség. De azt az adatvédelmi fetisizmust, ami a magyar jogi gondolkodásban megjelenik, nem lehet értelmes érvekkel védeni. A rossz szabályokat ki kell javítani, de ne a szabályozást, hanem a rossz szabályt okoljuk és javítsuk ki. Az adatvédelmi szabályaink egy 21. századi technikához rendelt NDK-s közigazgatásra épültek ki. Dobjuk ki az adatvédelmet? Nem hinném, hogy ez lenne a megoldás."[1]

Épp Magyarország – NDK-s közigazgatási behatásoktól egyébként mentes – huszadik századi történelme tragikusan bőséges példatára a személyes adatokkal való állami visszaéléseknek, például a legkülönfélébb diktatúrák alatti – az igazságosság fogalmával köszönőviszonyban sem álló – listázások útján, így ha valamit nem szükséges indokolni, az talán a személyes adatainknak az EU-ban valóban az egyik legszigorúbbnak mondható védelmének létjogosultsága. Más

[1] Nagy Marianna: *Interdiszciplináris mozaikok a közigazgatási jogi felelősség dogmatikájához*. Budapest, ELTE Eötvös, 2010. 130.

kérdés, hogy ennek intézményi formája még egyéni szinten sem volt teljesen egyértelmű, így fordulhatott elő, hogy amíg 2007-ben nem tűnt szükségesnek az adatvédelmi biztos hatáskörének további bővítése,

> „[…] hiszen a meglévő eszközök megfelelő mozgásteret biztosítanak, a jelenleg rendelkezésre álló hatáskörrel kell hatékonyan élnünk. Meggyőződésem ugyanakkor, hogy az adatvédelmi biztos a személyes adatok védelme, valamint a közérdekű adatok nyilvánossága érdekében akkor tud eljárni a jövőben is sikerrel, ha ombudsmani tekintéllyel tud fellépni, és az érintett szereplőkkel együttműködve munkálkodik a rá bízott jogok védelmén”,[2]

addig 2011-ben ugyanez a szerző már úgy vélte, hogy a „biztosi intézmény működése során bebizonyosodott, hogy mára már az ombudsmani hatáskör, eljárási rend és eszköztár nem teremt elegendő mozgásteret és lehetőséget az adatvédelmi jogsértések kivizsgálására és szankcionálására.”[3]

Érdemes azonban a lokális szemléletmód mellett egy olyan kitekintést is tenni, ami ha meglehetősen távolról indulva is, mégis hozzájárulhat az alapjogvédelem jövőbeli alakulásának külső körülményei jobb megértéséhez.

Magyary Zoltán az Amerikai Egyesült Államok közigazgatását, valamint alkotmányát vizsgálva azt találta, hogy az nem valamely elmélet, vagy államkonstrukció másolása útján alakította ki alkotmányos rendjét, hanem reálpolitikai érzékkel és politikai elméleti tudással érte el, hogy

> „[…] az Uniónak ne csak szuverenitása legyen olyan értelemben, hogy kötelező, az egész nemzetre irányadó határozatokat hozhasson és meghatározott kérdéseket törvényekkel szabályozhasson, amelyekre nézve az államoknak nincs szabad választása az elfogadás, vagy pedig az elvetés tekintetében, hanem az Uniónak közvetlen hatalma is legyen az állampolgárok felett, saját államaik kihagyásával.”[4]

---

2 Péterfalvi Attila: Az adatvédelem fejlődésének történeti áttekintése Magyarországon a GDPR hatálybalépéséig. In: Péterfalvi Attila (szerk.): *Szemelvények az információs jogok felügyeletének elmúlt 25 évéből*. Budapest, NAIH, 2020. 69. https://tinyurl.com/3f5nu8ke

3 Péterfalvi i. m. 71.

4 Magyary Zoltán: *Amerikai államélet – A közigazgatás útja az Északamerikai Egyesült Államokban*. Budapest, Királyi Magyar Egyetemi Nyomda, 1934. 17–18.

Geopolitikai megközelítésben még szembe ötlőbb lehet az (európai) uniós szintű végrehajtás tagállamokkal szembeni kieszközlésének nehézsége, miközben a nemzetközi prioritások nem a személyes adatok védelme, illetve általában sem az alapjogvédelem felé mutatnak az elmúlt évtized(ek)ben.

Brzezinski megközelítése államcentrikus,[5] tehát nem foglalkozik az Európai Unióval mint lehetséges politikai egységgel, azaz nem azonosítja azt geostratégiai játékosként, ugyanakkor regionális területi egységként sem releváns számára,[6] hiszen koncepciója szerint az csak valamely állam lehet.[7] Elképzelése értelmében az Európai Unió nem tekinthető önálló geostratégiai játékosnak, Franciaország és Németország azonban igen, miközben a tét az Eurázsia fölötti hatalom megszerzése és megtartása az Egyesült Államok által. Amerikai szempontból tehát az Európai Unióban kizárólag Franciaország és Németország releváns, míg „Ukrajna geopolitikai kulcsterületnek tekinthető, mivel független országként való puszta léte segít Oroszország átalakításában".[8]

Úgy tűnik, hogy az amerikai szemlélő – itt Kissinger személyében – valóban nehezen tudja az Európai Uniót geopolitikai realitásként elemezni *(„a hybrid, constitutionally something between a state and a confederation"*), ugyanakkor a német újraegyesítés értelmezhető számára, mert általa újra Németország lett a legerősebb nyugat-európai ország.[9]

Huntington, miközben arra az álláspontra helyezkedik, hogy a „világ eseményeinek főszereplői továbbra is a nemzetállamok",[10] úgy tűnik, hogy lemond az unipoláris világrend víziójáról és egy többpólusú, az egyes civilizációk egymás melletti létezése alapján álló világmagyarázatot kínál az olvasói számára, amit úgy nevez, hogy „civilizáció-központú paradigma"[11].

Ismeretes olyan álláspont is, ami szerint az EU globális aktorként látja magát.[12] Mivel az EU saját haderővel nem rendelkezik, ugyanakkor mégis formálni, befolyásolni kíván egyes globális folyamatokat, arra a következtetésre lehet jutni, hogy elsősorban a *soft power* lehet az az eszköz, amelynek útján ha-

---

5 Zbigniew Brzezinski: *A nagy sakktábla*. Budapest, Antall József Tudásközpont, 2017. 60.

6 Uo. 62.

7 Uo.

8 Uo. 72

9 Henry Kissinger: *World Order*. (Egyesült Királyság), Penguin Books, 2014. 92

10 Samuel P. Huntington: *A civilizációk összecsapása és a világrend átalakulása*. Budapest, Európa, 2006. 17.

11 Uo. 42

12 Bruno Maçães: *The Dawn of Eurasia – On the Trail of the New World Order*. (Egyesült Királyság), Allen Lane–Penguin Books, 2018. 52

tékonyan fel tud lépni. Természetesen számos más lehetőség is adódik, melyek közül az egyik, hogy ténylegesen is állammá alakul, és saját haderőt hoz létre és külpolitikai elképzeléseinek ezen az úton szerez érvényt, azonban jelenleg ez nem tekinthető reális forgatókönyvnek.

1.1. A GDPR mint globális soft power eszköz?

Elsőként azt szükséges hangsúlyozni, hogy a szakirodalom már ismeri a digitalizáció egyfajta gyarmatosításként *(digital colonization)* történő interpretációját.[13] Tovább gondolva ezt a megközelítést, úgy is kérdezhetnénk, hogy vajon egy technológiai újítás elterjedése következtében kialakított regionális szabályozás, aminek nem titkolt célja, hogy globális *arany standardként*[14] szolgáljon a világ többi része számára is, nem tekinthető-e önmagában egyfajta európai szabályozási gyarmatosításként?

Ugyanis az Európai Unió általános adatvédelmi rendeletét,[15] azaz a *GDPR*-t nem csak minden olyan EU-n kívüli szervezet (adatkezelő) köteles alkalmazni, amelyik az EU polgárainak személyes adatait kezeli, illetve az EU polgárai részére szolgáltatást nyújt, függetlenül attól, hogy ezt a tevékenységet földrajzilag hol fejti ki, feltéve, hogy rendelkezik az EU-ban letelepedett tevékenységi hellyel, hanem mindazon adatkezelők is, amelyek az EGT területén tartózkodó, bármely állampolgárságú személy személyes adatait kezelik.

Vagyis amennyiben valamely harmadik ország joghatósága alá tartozó vállalkozás az EU piacaira be szándékozik lépni, úgy nincs más választása, mint a GDPR rendelkezéseinek való teljes megfelelés biztosítása.

Csakhogy egyes multinacionális gazdasági szereplők a méretükből adódóan nem szívesen alakítják át üzleti modelljüket egy gazdasági integráció regionális szabályainak történő megfelelés érdekében. Amennyiben ezt az anyaországuk támogatásával teszik, úgy a regionális technológiai szuverenitás kialakítása, valamint a digitalizáció adatvédelmi szempontú szabályozásának érvényesí-

[13] Ld. pl. Danielle Coleman: Digital Colonialism: The 21st Century Scramble for Africa through the Extraction and Control of User Data and the Limitations of Data Protection Laws. *Michigan Journal of Race and Law,* Vol. 24. (2019). https://doi.org/10.36643/mjrl.24.2.digital

[14] Giovanni Buttarelli: *Privacy 2030. A New Vision for Europe*. IAPP, 2019. 23. https://iapp.org/resources/article/privacy-2030/

[15] 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) (EGT-vonatkozású szöveg), HL L 119., 2016.05.04., 1–88. o.

tése geostratégiai kontextussal bír. Nevezetesen azzal, hogy az Európai Unió önszabályozó gazdasági integrációként történő működése létező valóság-e, nem különben összeurópai föderációvá, azaz *de facto* politikai entitássá való átalakulása, illetve ennek elutasítása a saját tagállamainak a döntése lehet-e, vagy valamely külső nagyhatalom gazdasági, katonai, esetleg geopolitikai érdekeinek a függvénye-e.

Mindez első ránézésre talán szuverenitás-problémának tűnik, azonban sokkal inkább az a kérdés, hogy ki az erősebb geostratégiai játékos, azaz ki tudja a saját vízióit realizálni. Zbigniew Brzezinski sakktáblának[16] nevezi azt a területet (*Eurázsia*), amelynek egy részén terül el az Európai Unió.

Az első kérdés tehát az, hogy ki gyarmatosít kit? Az amerikai technológiai óriások gyűrik-e le anyaországuk teljes támogatásával az EU-t, vagy ellenkezőleg, az EU képes a saját földrajzi határain túl is jogi normái útján legalább részlegesen befolyásolni valamely globális megatrendet?

Ha Brzezinskit olvassuk, akkor egyértelmű, hogy amerikai szempontból az Európai Unióban kizárólag Franciaország és Németország tekinthető geostratégiai játékosnak. Alapvetően egyet lehet érteni Brzezinskivel, ami az EU tagállamai között Franciaország és Németország gazdasági jelentőségét, valamint geopolitikai ambícióinak realitását illeti. Ez azonban azt eredményezi, hogy Párizs és Berlin álláspontja a nagy amerikai technológiai óriásokról meghatározó az uniós adatvédelmi normák és a joggyakorlat alakításában.

Az első kérdés nyomán megfogalmazható a második is: vajon az uniós jogalkotás, különös tekintettel a GDPR elnevezésű termékére, tekinthető-e a *soft power*[17] egy eszközének,[18] figyelemmel arra, hogy amennyiben nem igazodik hozzá egy EU-n kívüli ország, úgy annak vállalkozásaival a tagállamok sokkal kevésbé valószínű, hogy üzletet fognak kötni, azaz szükségszerű piacvesztéssel járna a rendelet ignorálása? Tehát az uniós adatvédelmi kultúra még akár az olyan önkéntes recepcióra is alkalmas lehet, mint amilyen pl. a francia Code Napoléon *(Code civil des Français)* volt Latin-Amerikában.

Valamelyest relativizálja e kérdés létjogosultságát az amerikai technológiai óriások uniós jelenléte, hiszen napjainkban bár rekordösszegű közigazgatási bírságok kiszabására kerül sor, ezek az előre már beárazott bírságok egyelőre úgy tűnik, hogy továbbra is kifizetődővé teszik az EU jogával nem, vagy nem

16 Brzezinski i. m. 14.

17 Joseph S. Nye, Jr.: *Soft Power.* New York, PublicAffairs, 2004, x.

18 Uo. 75.

teljesen kompatibilis működésüket. E jelenség megalapozza a *soft power* fogalma kritikus értelmezését.

Ugyanis 2022-ben, illetve 2023-ban megtörténtek az első ilyen bírságkiszabások, miközben a GDPR már 2018. május 25-e óta kötelezően alkalmazandó valamennyi tagállamban, másrészt sajátos jelenség, hogy a nagy technológiai óriások Írországban telepedtek le, azaz az ír adatvédelmi hatóság jogosult – és köteles – eljárni ezen vállalkozások jogsértő adatkezelése esetén. Valamilyen megfontolásból azonban az ír hatóság nem szerzett érvényt a közösségi jognak, aminek a vége az lett, hogy az Európai Adatvédelmi Testület volt kénytelen több kötelező erejű döntést hozni, amelyekben nem csak kötelező döntéshozatalra utasította az ír hatóságot, hanem a döntés tartalmát is meghatározta.

Ebből szükségszerűen következik az a megállapítás, hogy 1) hiába kötelező egy norma alkalmazása, amennyiben azt egy tagállam vonakodik végrehajtani, úgy a jogi eszköz csupán elméleti lehetőségként létezik, de nem tényleges eszköze valamely közösségi érdek érvényesítésének; 2) amennyiben egyes – főleg globális befolyással nem bíró, kisebb – igazgatottakkal szemben kellő visszatartó ereje lehet egy normának, ám a tagállami hatóságok épp azon technológiai óriásokkal szemben nem tudnak érvényt szerezni még bírságolás útján sem e normának, amelyekkel szemben elsődlegesen meg lett alkotva, úgy nem csak a *soft power*, hanem egyáltalán mint jogi norma minősége is relativizálódik, azaz lesznek olyan kevésbé befolyásos jogalanyok, amelyek nem tudják megkerülni az alkalmazását, és lesznek olyanok, amelyek eleve olyan tagállamban telepednek le, amelynek hatóságai nem kellő szigorral kérik számon rajtuk a közösségi szabályokat.

Ez azonban a szabályozás uniós szintje miatt azt jelenti, hogy amennyiben a letelepedés helye szerinti adatvédelmi hatóság, mint fő felügyeleti hatóság nem jár el, vagy egyszerűen nem hoz határozatot az adatkezelővel szemben, úgy hosszas vitarendezési eljárás szoríthatja csak rá a tagállami hatóságot a rendelkezések érvényesítésére. Ám a bírság egyszeri kiszabása továbbra sem garantálja a jogkövető magatartás sikeres és tartós kikényszerítését. Vagyis bizonyos gazdasági méret már olyan befolyást eredményez, ami a jogi normák hatékony alkalmazhatóságát is megkérdőjelezi.

Erre tekintettel külön igazolásra szorulna, hogy a GDPR kötelező alkalmazása tekinthető-e a *soft power* eszközének, illetve amennyiben igen, úgy mely jogalanyokkal szemben igen és melyekkel szemben nem.

A harmadik kérdés pedig szintén megfogalmazható az azt megelőző alapján: amennyiben a GDPR-t a *soft power* egyik lehetséges eszközeként határoznánk meg, úgy egy gazdasági integráció, tehát egy állami entitásnak nem tekinthető

regionális szereplő valóban képes-e a jogi normát a hatalom ilyen gyakorlásaként alkalmazni, vagy *de facto* az erősebb tagállamok (Franciaország, Németország) eszközeként, de közösségi köntösbe bújtatva funkcionálhat-e inkább? Az így megfogalmazott kérdés esetén is kétséges azonban, hogy az EU, illetve EGT határain túl, önkéntes recepció útján, azaz valóban *soft power* jelleggel tudjon érvényesülni az európai adatvédelmi jogi rezsim a nagy online platformok világában.

1.2. Közbenső következtetések

Az előzőekben megfogalmazott kérdések alapján legalább három közbenső következtetés fogalmazható meg.

Egy önálló államiság nélküli, pusztán gazdasági integráció nem képes az egyes államokra jellemző tevékenységekre, azonban az Európai Unió az uniós polgárság intézményének bevezetésével már nem kizárólag gazdasági szereplő, hanem a hatásköreire is tekintettel egyre inkább *állami jelleget ölt*. Ebből adódóan további vizsgálódás nélkül nem jelenthető ki, hogy az Európai Unió legalább elméletileg ne lehetne képes a saját adatvédelmi jogi rezsimjét egyfajta, jogi értelemben vett globális kolonizáció szolgálatába állítani.

Feltételezhető, hogy a GDPR alkalmazása alkalmas az EU piacaira való bejutást megkönnyíteni egyes szektorokban, míg annak elutasítása a közösségi piacokhoz való hozzáférést akadályozza, vagy teljesen ki is zárja.

Erre tekintettel nem zárható ki, hogy az általános adatvédelmi rendeletnek való megfelelőség tagállami hatóságok, illetve az EU intézményei általi megállapítása a *soft power* eszközének tekinthető. Álláspontom szerint egyes vállalkozások, illetve államok esetében a GDPR akár a *soft power* eszközeként is interpretálható, de külön kategóriát képeznek azok a méretüknél, vagy a világgazdaságban betöltött szerepüknél fogva fajsúlyos globális szereplők, amelyek képesek az adatvédelmi jogi követelményeket megkerülni, vagy bevételeikre tekintettel egészen egyszerűen előre ‘beárazzák’ a jogsértéseket, és még így is megéri nekik az uniós jog részleges megkerülésével működniük az EU területén.

A *soft power* egyik eszközeként interpretált uniós adatvédelmi jog (GDPR) esetében indokolt megvizsgálni, hogy kinek áll hatalmában ezt az eszközt a gazdasági élet szereplőivel szemben alkalmazni, és milyen célból, illetve azt is, hogy ennek mi értelme lehet, milyen célt szolgálhat egy ilyen jogi eszköz általánossá tétele.

Feltételezhető, hogy az EU csak korlátozott mértékben képes érvényre juttatni EU-n kívüli országokkal és azok gazdasági szereplőivel szemben a GDPR egyes rendelkezéseit, ezért elsősorban az egyes tagállamok képesek hatékonyan alkalmazni az adatvédelmi szabályokat.

Ebből következően feltételezhető továbbá, hogy elsősorban a gazdaságilag (is) erős tagállamok képesek a *soft power* eszközeként alkalmazni a GDPR-t.

2. A GDPR végrehajtásának egyes aktuális jogi kérdései a magyar közigazgatás szempontjából

2.1. Uniós rendeleti szintű adatvédelem – *privacy* helyett *data protection*

2018. május 25. jelentős mérföldkő a hazai, de egyébként az uniós adatvédelmi jog számára is. Ettől kezdve ugyanis kötelezőek és közvetlenül alkalmazandóak a GDPR-ban meghatározott adatvédelmi jogi minimumkövetelmények.

A GDPR 51. cikkének (1) bekezdése előírja, hogy a „rendelet alkalmazásának ellenőrzéséért egy vagy több független közhatalmi szerv (felügyeleti hatóság) felel". Ezt az előírást Magyarországon az Infotv.-nek a csak 2018. július 26. napjától hatályos 38. § (2a) bekezdése útján teljesítette a hazai jogalkotó, amikor a NAIH-ot nevezte meg kijelölt hatóságként.

A GDPR szakított az addig töretlen, *privacy*-alapú adatvédelmi megközelítéssel, amelynek a *common law*-ból eredő gyökerei visszanyúlnak Warren és Brandeis ma már klasszikusnak számító cikkéig.[19] A már nem hatályos 95/46/EK irányelv 1. cikkének (1) bekezdése még kifejezetten „a magánélet tiszteletben tartásához való jogukat a személyes adatok feldolgozása tekintetében" szófordulatot tartalmazta, ezzel az angol *privacy* fogalmát a magánélettel azonosítva.

Ezzel szemben a GDPR már nem hivatkozik a *privacy* fogalmára.

A hazai szakirodalom a személyes adatok védelmét továbbra is mint információs önrendelkezési jogot értelmezi:

> „Az Alkotmánybíróság tehát az Alaptörvény alapján is a személyes adatok védelméhez való jogot nem hagyományos

[19] Samuel D. Warren – Louis D. Brandeis: The Right to Privacy. *Harvard Law Review,* Vol. 4, No. 5. (1890) 193–220.

> 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."[20]

Az információs önrendelkezési jogként definiált adatvédelemhez való jog koncepciója tekintetében azonban egyáltalán nem vagyok meggyőződve arról, hogy a közigazgatási típusú adatvédelem gyakorlata hosszú távon összeegyeztethető marad az alkotmánybírósági értelmezéssel. Ennek oka pedig a személyes adatok gazdasági célú, sokszor nagy adatbázisok *(big data)* és mesterséges intelligencia útján történő felhasználása, amely esetekben nem szükségszerű, hogy az érintettek hozzájárulásukat adták személyes adataik kezeléséhez, illetve ha ezt tették sem biztos, hogy az önkéntes elem maradéktalanul megvalósult.

Véleményem szerint a technikai és gazdasági valóság részben már meghaladottá tette az információs önrendelkezési jogként történő értelmezés társadalmi kontextusát. A jogalkotás, a közigazgatás és főleg a jogtudomány ettől még ragaszkodhat az önrendelkezési jog hagyományossá vált alkotmányjogi koncepciójához, de a magyar közigazgatás *de facto* nem bír ráhatással a határain túl, és különösképpen az EU-n kívül folyó személyes adatkezelésekre, így külföldi adatkezelővel szemben érintetti kérelemre sem fog tudni tényleges jogvédelmet nyújtani.

Mindenesetre a legújabb európai szakirodalom az EUB esetjogát elemezve már egyértelműen különbséget tesz, például a GDPR 25. cikke által nevesített beépített és alapértelmezett adatvédelem körében, a *privacy* és a *data protection* (adatvédelem) fogalma között.[21]

2.2. A közigazgatási szankciók

Az adatvédelmi hatósági eljárások legerősebb szankciója jelenleg az adatvédelmi, másképp közigazgatási bírság. Emellett 2022. január 1-jétől hatályos

[20] Sulyok Tamás – Villám Krisztián – Deli Gergely: A személyes adatok védelme az Alkotmánybíróság gyakorlatában. In: Szabó Endre Győző (szerk.): *Az Infotörvénytől a GDPR-ig.* Budapest, Ludovika, 2021. 46.

[21] Lee A. Bygrave: Article 25. Data protection by design and by default. In: Christopher Kuner – Lee A. Bygrave – Christopher Docksey (szerk.): *The EU Data Protection Regulation (GDPR).* Oxford, Oxford University Press, 2020. 575. https://doi.org/10.1093/oso/9780198826491.001.0001

az Infotv. 61. §-ának azon módosítása, amely a korábbiakhoz képest érintetti kérelem hiányában is lehetővé teszi a jogellenesen kezelt személyes adatoknak a hatóság által meghatározott módon végrehajtandó törlése elrendelését. A törvénymódosítás bár az Alkotmánybíróság 3110/2022. (III. 23.) AB határozatával összhangban áll, tulajdonképpen ennek hiányában is megállapítható volt számára az e szankció hatóság általi alkalmazásának jogszerűsége.

Jelen tanulmányban a GDPR szankciórendszeréből a közigazgatási bírság alkalmazásának egyes kérdésein keresztül igyekszem az egységes tagállami végrehajtással kapcsolatban észrevételeket tenni.

A GDPR 83. cikke eddig is részletesen rendelkezett a közigazgatási bírság kiszabásának általános feltételeiről, azonban az EDPB 04/2022. sz. iránymutatása az általános adatvédelmi rendelet szerinti közigazgatási bírságok kiszámításáról[22] tovább részletezi a bírságösszeg kiszámításának lehetséges szempontjait.

A bírság iránymutatás, számos újdonsága mellett egy ötlépcsős módszertant vezetett be. Az első lépcső szerint az adatkezelési műveleteket szükséges azonosítani, és a GDPR 83. cikkének (3) bekezdése szerint értékelni. A második lépcsőben a bírságkalkulációhoz szükséges kiindulópontot kell meghatározni a 83. cikk (4)–(6) bekezdéseinek azonosításával, a jogsértés súlyosságának értékelésével, tekintettel a 83. cikk (2) bek. a)-b), valamint g) pontjaira, valamint a kötelezett vállalkozás árbevételének értékelésével, arra figyelemmel, hogy a kiszabásra kerülő bírság arányos legyen és kellő visszatartó erővel bírjon. Harmadik lépésben az enyhítő és súlyosító körülmények értékelése útján az iránymutatás mellékletben található táblázataiban található határok között a bírságösszeg növelése vagy csökkentése történik. Negyedik lépcsőben a tárgyi üggyel érintett adatkezelési műveletekre meghatározott bírságmaximumot szükséges megállapítani. Végezetül az iránymutatás szerint a bírság összegének hatékonysága, visszatartó ereje és arányosságának értékelése következik, amely lehetővé teszi a bírságösszeg végleges kiigazítását.

Amennyiben a GDPR szankciórendszerének talán e legerősebb elemét valóban minden tagállami hatóság egyöntetűen alkalmazná, akkor valóban egységes uniós végrehajtás valósulna meg e téren, és ez feltehetőleg fokozott adatvédelmi tudatosságra ösztönözné az adatkezelő vállalkozásokat. Ugyanakkor az iránymutatás szerint: „Ez nem sérti a nemzeti hatóságok azon hatáskörét, hogy bírságot szabjanak ki a természetes személyekre.” (04/2022. sz. iránymutatás, 1.3.)

[22] 04/2022. sz. iránymutatás az általános adatvédelmi rendelet szerinti közigazgatási bírságok kiszámításáról. 2.1. változat. European Data Protection Board, 2023. május 24. https://tinyurl.com/2ukx3522

Így tehát a természetes személy adatkezelők vonatkozásában továbbra is jelentős tagállami eltérések fognak érvényesülni. Továbbá kérdéses, hogy ha a bírságösszegek uniós szinten uniformizálásra, de legalábbis jelentős közelítésre kerülnek, úgy a különböző adókulcsokkal, GDP-vel, gazdasági stabilitással, vagy éppen normakövetési hajlandósággal bíró tagállamok gazdasága számára valóban azonos következményekkel fog-e járni ez a megoldás.

2.3. Közigazgatási büntetőjog?

A bírság iránymutatáson túl érdemes röviden áttekinteni az EUB két, 2023 decemberi döntését, amelyek érintik a GDPR 83. cikk (2) bek. b) pontja alapján már eddig is alkalmazandó szempontot, azaz közigazgatási bírság kiszabása esetén a jogsértés szándékos vagy gondatlan jellegének megállapítását, amit a tagállami hatóságok eddig nem minden esetben vettek hangsúlyosan figyelembe.

2.3.1. A vétkességen alapuló felelősség közigazgatási bírság esetén

A C-683/21. sz., 2023. december 5-i ítéletében[23] az EUB nagytanácsa előzetes döntéshozatali eljárás keretében többek között azt elemezte egy litván közbeszerzés nyomán megvalósult adatkezelés jogellenessége miatt a litván adatvédelmi hatóság által kiszabott közigazgatási bírság kapcsán, hogy kizárólag szándékos vagy gondatlan elkövetés esetén szabható-e ki adatvédelmi bírság. A litván kormány és az Európai Unió Tanácsa szerint a 83. cikkből kiolvasható egyfajta tagállami mozgástér [62. pont], azonban az EUB ítélete szerint ez az értelmezés nem fogadható el [63. pont], azaz kizárólag arra van a tagállamoknak lehetőségük, hogy azt eldöntsék, hogy közfeladatot ellátó szerveikkel szemben is kiszabható-e és milyen mértékű közigazgatási bírság [68. pont] – Magyarországon például 20 millió forint bírságösszegig igen –, azonban ezen túlmenően, kifejezetten anyagi jogi feltételeket a tagállamok nem írhatnak elő [69. pont]. Tehát a 83. cikk autentikus értelmezése alapján nincs olyan tényező, amely arra utalna, hogy „az adatkezelő vétkes magatartása hiányában megállapítható lenne az adatkezelő felelőssége" [71. pont], [79-80. pont],

[23] C-683/21. sz. ügy, a Vilniaus apygardos administracinis teismas (vilniusi megyei közigazgatási bíróság, Litvánia) által benyújtott előzetes döntéshozatal iránti kérelem tárgyában [ECLI:EU:C:2023:949].

vagyis kizárólag a GDPR rendelkezéseinek vétkes megsértése alapozhatja meg az adatvédelmi bírság kiszabását [73. pont].

Az EUB döntése tehát az objektív felelősséget adatvédelmi jogsértés esetén történő közigazgatási bírság kiszabása során kizárja, a szankció csakis vétkességen alapulhat, ennek – helyes – megállapítása pedig a tagállami adatvédelmi hatóság feladata és felelőssége.

A közigazgatási bírság büntetőjogias jellegére utal, hogy amint azt az EUB hangsúlyozta, a 83. cikk (2) bekezdésének a (3) bekezdésével összefüggésben történő értelmezése „a rendelet halmazatban történő megsértésének következményeiről rendelkezik", azaz az egy cselekménnyel elkövetett több vétkes jogsértés esetén sem szabható ki a bírságmaximumnál nagyobb közigazgatási bírság [72. pont].

Az EUB azt is kifejtette, hogy mit ért vétkesség alatt az adatkezelők vonatkozásában: „amennyiben tudatában kellett lennie magatartása jogsértő jellegének, akár tisztában volt azzal, akár nem, hogy megsérti az általános adatvédelmi rendeletben foglalt rendelkezéseket" [81. pont]. Egyidejűleg azt is kifejtette az EUB, hogy amennyiben az adatkezelő jogi személy – amint az előzetes döntéshozatallal érintett litván adatkezelő is – úgy a rendelet 83. cikkének alkalmazása „nem feltételezi az adott jogi személy irányító testületének részvételét, vagy erről való tudomását" [82. pont].

Ez álláspontom szerint azt eredményezi, hogy bár a jogi személynek „tudatában kellett lennie" a jogsértő jelleggel, függetlenül attól, hogy képviselői, illetve vezetői tudtak-e a jogsértő cselekmény bekövetkezéséről, tehát elméletileg vétkességen alapul a jogi felelősség, valójában mégis inkább tűnik objektívnek, hiszen egy gazdálkodó szervezet az adatkezelése megkezdését megelőzően kell hogy átgondolja annak minden későbbi részletét, ami eleve nagy terhet jelent például a kkv-k esetében, de ha később egy alkalmazott jogsértően jár el, úgy ezért az adatkezelő jogi személy felel, kivéve, ha bizonyítja, hogy nem volt tudatában magatartása jogsértő jellegének, amely nem leges bizonyítás jogi személy esetében legalábbis nehezen értelmezhető.

2.3.2. A német szabálysértési törvény mint a GDPR 83. cikke szerinti közigazgatási bírság kiszabásának alapja?

A C-807/21. sz.,[24] szintén 2023. december 5-i ítéletében az EUB nagytanácsa előzetes döntéshozatali eljárás keretében többek között azt vizsgálta, hogy elfogadható-e a 83. cikk szerinti közigazgatási bírság kiszabásának előfeltételeként, ha a tagállami jog, jelen esetben a német szabálysértési törvény rendelkezése szerint előbb a jogi személy jogsértő cselekményét be kell tudni egy azonosított természetes személynek, és ezt követően történik a bírság kiszabása.

Az EUB álláspontja szerint az ellentétes a 83. cikk (1) bekezdésével [51. pont], továbbá az EUMSZ 288. cikk második bekezdésével is, hiszen a rendelet kötelező és közvetlen hatállyal bír minden tagállamban [52. pont].

A továbbiakban ezen ügyben is a vétkességen alapuló jogsértés körülményeit vizsgálta az EUB. Mivel a GDPR 83. cikke nem mondja ki explicite, hogy jogi személy adatkezelő esetén közigazgatási bírság kizárólag akkor szabható ki, ha a jogsértést szándékosan vagy gondatlanul követte el, a német, az észt, valamint a norvég kormány, továbbá az Európai Unió Tanácsa úgy látta, hogy bizonyos mérlegelési mozgástere maradt a tagállamoknak [62-63. pont]. Az EUB értelmezése szerint azonban „ilyen értelmezésnek nem lehet helyt adni" [64. pont].

Az ítélet a továbbiakban az előző pontban ismertetett litván üggyel azonos érvelést alkalmaz, kiemelve, hogy a GDPR egyszerre irányul egyenértékű és egységes védelmi szintre, a GDPR 83. cikkét az EU egész területén következetesen kell alkalmazni, így a vétkességen alapuló felelősségtől eltérő tagállami szabályozás ellentétes lenne e céllal, továbbá „torzíthatná a gazdasági szereplők közötti versenyt az Unión belül" [74. pont].

2.3.3. Tagállami közigazgatási büntetőjog határon átnyúló egységes végrehajtás útján?

Nagy Marianna már idézett művében, 2010-ben Kis Norbertre hivatkozott, amikor megállapította, hogy írásai

> „[…] egy még szorosabb büntetőjogi kapcsolódás iránti igényt vetnek fel, részben a szupranacionális jog érvényesítésére

[24] C-807/21. sz. ügy, a Deutsche Wohnen SE és a Staatsanwaltschaft Berlin között folyamatban lévő eljárásban benyújtott előzetes döntéshozatal iránti kérelem tárgyában [ECLI:EU:C:2023:950].

> vonatkozóan, hiszen a közigazgatási büntetőjog fogalmába beleérti az Európai Unió jogának érvényesítésére vonatkozó szankciókat is, […] a közigazgatási jogérvényesítést, szinte a teljes szankciórendszert csakis felelősségi alapon képzeli el."[25]

Nagy Marianna álláspontja szerint a szabálysértési szankciók „szigorúan szubjektív alapú szankciók, mégpedig egy kompakt büntetőjogi bűnösségi logikán belül a szándékosság-gondatlanság fogalompárra épülnek."[26]

Az EUB előző pontban ismertetett döntései is a szubjektív alapú szankció jogdogmatikai fogalmának irányába mutatnak, sőt, a német jogeset alapvetően büntetőjogias jelleget mutat, amennyiben a német szabálysértési törvény alkalmazását is a GDPR, valamint az EUMSZ egyes rendelkezéseibe ütközőnek tartja az ítélet, ezzel a vétkesség fogalmának büntetőjogi értelmezése felé orientálva a tagállami jogalkalmazó hatóságokat.

Mustert az Európai Bizottság GDPR-t végrehajtó rendelet-tervezetét elemzi és rávilágít, hogy a Bizottság szerint a GDPR egységes végrehajtását jelenleg a tagállami hatóságok eltérő hatékonyságú eljárásjogi normái veszélyeztetik a határokon átnyúló ügyekben.[27] Nem az elemzés hiányossága, hanem a Bizottság tervezetéé a tagállami szintű ügyek egységes színvonalú elbírálásának igényéről való teljes hallgatás. Ennek az az üzenete, hogy a tagállami polgárok a határon át nem nyúló adatkezelések vonatkozásában továbbra is a saját államuk által nyújtott szintű adatvédelemben fognak részesülni.

Mustert többek között bemutatja, hogy tagállamonként különböző módon viszonyulnak az egyes hatóságok a kérelmekhez. Luxemburgban a kérelem benyújtása előtt az adatkezelőhöz szükséges fordulni, Ausztriában pedig elévülési ideje van a panasz benyújtásának, míg Hollandiában kizárólag az érintett nyújthat be kérelmet az adatvédelmi hatósághoz.[28]

Azt kiegészítésként hozzátehetjük, hogy Magyarországon bár sem az adatkezelő előzetes megkeresése, sem elévülési határidő nem akadályozza a hatóság előtti jogérvényesítést, azonban ha valaki nem az adatkezelés érintettjeként fordul a hatósághoz, úgy kizárólag az Infotv. szerinti ún. 'ombudsmani típusú' eljárást, azaz vizsgálatot kezdeményezhet, ami egyfokú (közigazgatási)

---

25 Nagy i. m. 23.

26 Uo. 39.

27 Lisette Mustert: The Commission Proposal for a New GDPR Procedural Regulation: Effective and Protected Enforcement Ensured? *European Data Protection Law Review,* Vol. 9, Issue 4. (2023) 454. https://doi.org/10.21552/edpl/2023/4/12

28 Uo. 455.

eljárás, bírói jogorvoslat nélkül és bár van törvényes ügyintézési határidő, de annak elmulasztása esetén mulasztási per sem kezdeményezhető (sőt, sajátos módon még az Ákr. szerinti közigazgatási hatósági eljárás esetén is a hatóság rendelkezésére álló eljárási határidő elmulasztásától számított egy éven belül kezdeményezhető mulasztási per, az azon túl előterjesztett kereseti kérelmet a perre illetékes Fővárosi Törvényszék elutasítja). Csehországban pedig még ha maga az érintett fordul is a hatósághoz, a kérelmet megvizsgálva a hatóság dönti el a beadvány vizsgálata nyomán, hogy indít-e hivatalból hatósági eljárást, vagy sem. Ez utóbbi esetben pedig még ombudsmani típusú eljárást sem tud kérni az adatalany.

Az egységes tagállami végrehajtás kapcsán a Bizottság továbbá nem vizsgálta, hogy tagállamonként eltérő a végrehajtásért felelős hatóság típusa, beleértve, hogy van tagállam, ahol a hatóság ombudsmant és a hivatalát jelenti. Ugyanígy az egységes végrehajtás megvalósíthatóságát kérdőjelezi meg a tagállamonként eltérő mértékű hatósági költségvetés, személyzet, valamint informatikai támogatás.

Mindezen körülmények pedig arra világítanak rá, hogy egy rendelet végrehajtási szabályainak hiányosságait egy újabb rendelettel lehet ugyan szűk körben, jelen esetben a határokon átnyúló személyes adatkezelések vonatkozásában egységesíteni, azonban épp tagállami szinten, az EU polgárainak többsége számára semmilyen előrelépést sem fog jelenteni személyes adataik védelméhez fűződő alapvető joguk érvényesítése tekintetében.

3. Összegzés

Bár a személyes adatok védelme az Európai Unióban a tagállami hatóságok végrehajtásán keresztül valósul meg főszabályként, az tapasztalható, hogy a digitalizáció mint megatrend nincs tekintettel a közösségi szabályozás tagállami szintű, országonként eltérő végrehajtási mechanizmusaira. Ugyanígy kijelenthető, hogy a geopolitikai események sodrásában egyedi kísérlet az EU jog- és értékrendjének békés úton történő, akár *soft power* eszközként is értelmezhető terjesztése, azonban figyelembe kell venni az eurázsiai térséget mozgató nagyhatalmi ‘játszmákat’ is, amelyek nem csak az EU esetleges bővítését, de az egész nyugati civilizáció földrajzi kiterjedését meghatározzák.

Ebben a kontextusban vizsgálva a GDPR végrehajtását, arra a következtetésre lehet jutni, hogy az általa meghatározott szankciórendszer, így az annak részét

képező közigazgatási bírság hatékony alkalmazása esetén is több a kérdőjel, semmint az egységes közösségi fellépést empirikusan alátámasztó tény.

Rövid távú megoldásként észszerűnek tűnhet tehát egy uniós szintű végrehajtási rendelet kibocsátása, azonban amennyiben ez nincsen tekintettel a tagállami polgárok mint igazgatottak helyi szintű jogsértéseinek kivizsgálására, hanem csak a határokon átnyúló személyes adatkezelések vonatkozásában tartalmaz egységes eljárási szabályokat, úgy a közigazgatásba, valamint ez EU intézményrendszerébe és alapjogvédelmének hatékonyságába vetett bizalom tovább csorbulhat.

Ennek a helyzetnek az orvoslása azonban nem a tagállamok adatvédelmi hatóságainak a GDPR rendelkezései végrehajtásában rejlő kötelezettsége, hanem a tagállami, valamint az uniós jogalkotók együttes felelőssége.