Szabó Endre Győző

A védelmi lépcső elmélete

LUDOVIKA
EGYETEMI KIADÓ

Szabó Endre Győző

A védelmi lépcső elmélete

Vákát

Szabó Endre Győző

A védelmi lépcső elmélete

A GDPR védelmi szintjének elemzése

LUDOVIKA
EGYETEMI KIADÓ
Budapest, 2022

Szakmai lektor:
Váradi Szilvia

A kézirat lezárásának időpontja:
2020. július 23.

Kiadja a Nemzeti Közszolgálati Egyetem
Ludovika Egyetemi Kiadó
A kiadásért felel: Deli Gergely rektor

Székhely: 1083 Budapest, Ludovika tér 2.
Kapcsolat: kiadványok@uni-nke.hu

Felelős szerkesztő: Benkő Krisztina
Olvasószerkesztő: Tomka Eszter
Korrektor: György László
Tördelőszerkesztő: Fehér Angéla

Nyomdai kivitelezés: Gelbert ECO Print Kft.
Felelős vezető: Gellér Róbert

DOI: https://doi.org/10.36250/01031_00

ISBN 978-963-531-777-6 (nyomtatott)
ISBN 978-963-531-778-3 (ePDF) | ISBN 978-963-531-779-0 (ePub)

Az Unió az emberi méltóság tiszteletben tartása, a szabadság, a demokrácia, az egyenlőség, a jogállamiság, valamint az emberi jogok – ideértve a kisebbségekhez tartozó személyek jogait – tiszteletben tartásának értékein alapul.

Az Európai Unióról szóló szerződés 2. cikkének
első mondata

Vákát

Tartalom

Vákát

Előszó

A védelmi lépcső elmélete című kötet megjelenése örömmel tölt el, jó látni, hogy egy sokéves vállalás, a doktori értekezés megírása, majd önálló kötetben publikálása valósággá válik. Az elemző munka, amelyet a szerző az értekezésében elvégzett, sok szálon kötődik a munkámhoz és érdeklődésemhez. A személyes adatok védelméhez fűződő jog egyike a nehezen megfogható, körülhatárolható alapjogoknak. Ennek egyik oka valószínűleg abban keresendő, hogy a viszonylag fiatal, harmadik generációs jognak sok másikkal összevetve kevesebb az elméleti megalapozottsága. Az alkotmányjogi összefüggésen túl uniós jogi érdeklődésem miatt is jó szívvel veszem kezembe a kötetet, amely a szinte már misztikusnak ható általános adatvédelmi rendelet, a GDPR pragmatikus elemzését adja.

Kötődésem a kötethez, a témához, az elvégzett munkához személyes is. Nem csupán arra az élményemre gondolok, amikor a nyilvános védés alkalmával ünnepélyes keretek között egyhangúan javasoltuk az értekezés elfogadását és a fokozat megadását. A dolgozat mögötti személyes munka ismerős a számomra. Ismerős a jogász, az értelmiségi vívódása, hogy az a munka, amelyet végzünk, vajon elég hatékony-e? Jól gazdálkodunk-e az időnkkel, tehetségünkkel, erőforrásainkkal? Eleget teszünk-e a jogászi hivatással együtt járó feladatunknak, ahol a hétköznapi tapasztalatból szabályozás iránti igény, majd jogszabály lesz, és a hivatalos közlönyben megjelenő fekete-fehér szövegből a jogkeresők számára helyes döntéseket várnak el? Ez a törekvés végigkísér bennünket a jogászi pályán. Az értekezésben körüljárt kérdések, a különböző védelmi szintek összehasonlítására tett javaslat, a védelmi lépcső gondolata mind ebből a jogászi alapállásból indulnak ki.

Amikor 2014. szeptember 22-én az Országgyűlés illetékes bizottsága alkotmánybíró-jelöltként meghallgatott, a jogállammal összefüggésben úgy fogalmaztam, hogy *„a legapróbb egyéni jogsértés se maradjon megfelelő alkotmányjogi következmény nélkül, és ez megerősíti a polgárok hitét a jog nemzetet szervező és nemzetet megtartó erejében”*. A szerző, Szabó Endre Győző is osztja ezt a célkitűzést. Meggyőződésem, hogy a kötet olyan tudományos eredmény, amelyet nem csak napi teendőink során vehetünk le a polcról tájékozódás céljából. Azt az üzenetet is hordozza: feladatom volt, és ezt el is végeztem. Jó érzéssel írhatjuk le ezt.

A szerzőt ismerve biztos vagyok abban, hogy továbbhalad a megkezdett úton, és további írásaival fogja értelmezni, elemezni és közelebb hozni az adatvédelem elméleti és gyakorlati kérdéseit az olvasóhoz.

Dr. Sulyok Tamás
az Alkotmánybíróság elnöke

A szerző előszava

Az olvasó a 2020 szeptemberében megvédett doktori értekezésemet tartja a kezében. A kéziratot 2020 júliusában lezártam. Az eredeti változathoz képest minimális korrekciókat végeztem a szövegen ott, ahol ez a kézirat minőségének javítása érdekében szükséges volt.

A PhD-kutatásom mögött az a kérdés állt, vajon hogyan lehet kikerülni az alacsony hatásfokú jogérvényesítés és jogérvényesülés csapdájából. Ahhoz, hogy ezekről a kérdésekről és kételyekről előremutató párbeszédet folytathassunk, megalapozó munkák szükségesek. A GDPR védelmi szintjének elemzése és a különböző védelmi szintek közötti lehetséges különbségek feltárására irányuló munkám ebben a szellemben született.

Az adatvédelemhez való jog az emberi méltóságnak a magánszférát érintő aspektusához tartozik. E jog érvényesülését az alapelvektől a technikai részletekig menő jogszabályok szolgálják. Ha a személyes adatok védelméről értekezünk, magától értetődik, hogy magas szintű védelemről szólunk, vagy legalábbis azt tekintjük célnak. Amikor itt, az előszóban alacsony szintű védelemről beszélek, akkor nem csupán a védelem hétköznapi értelemben vett jelentését hiányolom. Meg kell nyitnunk egy ennél tágabb perspektívát, ez pedig az adatvédelmi kultúrát jelenti.

Számomra az adatvédelmi kultúrát leginkább azok a hétköznapi magatartások jellemzik, amikor az emberi méltóság érvényesül, amikor az érintettek azt élhetik meg, hogy az adatvédelmi szabályok tiszteletben tartása révén ők maguk is figyelmet, tiszteletet kapnak, tehát a védelem érvényesül. Minden olyan magatartás, amely ebbe az irányba mutat, ennek feltételeit teremti meg, az adatvédelmi kultúrát szolgálja.

Én magam lassan két évtizede a hatósági gyakorlat területén dolgozom. Természetesnek tűnt egy idő után, hogy a tudomány irányába forduljak. Azok közé tartozom, akik a gyakorlati munka mellett kivehetik a részüket az oktatásból, tankönyvek fejlesztéséből, publikációk írásából, vizsgáztatásból.

A gyakorlat és a tudomány területén természetes szövetség jön létre, egyszersmind hiányokkal is szembesülünk. Ismét hiányokról írok – de mi hiányzik a mai magyar tudományos életből az adatvédelem területén? Hiányként említhetjük az adatvédelmi tanszékeket az egyetemeken, hiányolhatjuk a téma nagy professzorait, akik talán már élnek, de még nem futották be azt a pályát, amelyre olyan nagy szükség lenne. Hiányolom

a szakmai folyóiratot, ahogyan az adatvédelmi szakkönyvtárat is. A tudomány sok mindent hozzátehetne tehát az adatvédelmi kultúra erősítéséhez.

Akkor, amikor szűkös szabadidőmben a tudományos munkához teszek hozzá egy kicsit, mindig azt érzem: egy kis hiányt pótoltam, egy kis adósságot törlesztettem az adott munkával. Így vagyok a doktori értekezésemmel, és annak publikációjával is.

Bízom abban, hogy az írásom hasznosnak bizonyul mindazoknak, akik azzal a céllal veszik kézbe, hogy az adatvédelemmel szorosabb barátságot kössenek. Amikor újra végigolvastam a kéziratot, az a remény fogalmazódott meg bennem, hogy ez az új kötet tankönyvként is megállhatja a helyét. Az idő majd eldönti. Akárhogy lesz is, jó érzéssel zártam le ezt a kötetet, és ezzel együtt egy szakaszt is a szakmai pályámon.

Kívánom minden olvasónak, hogy a sorok között mindig ismerje fel az egyéni sorsot, amit a jog véd, és a közjót vagy közérdeket, amit a jog megfogalmazni próbál. Végső soron ezért dolgozunk, ezért van értelme a mindennapi munkánknak, és így lehetünk majd talán elégedettek, amikor évtizedek múltán visszatekintve azt mondhatjuk: mi is hozzátettünk valamit az adatvédelmi kultúra építéséhez.

Szabó Endre Győző

Bevezetés

A természetes személyekhez kötődő információk védelme, vagyis az adatvédelem az utóbbi évtizedekben az emberi méltóság védelmének egyik aspektusaként jelent meg a jogi gondolkodásban.

A személyes adatok védelmének anyajoga az emberi méltóság.

> Az európai kontinentális jogfejlődésben ez a kijelentés teljesen természetes. Figyelemre méltó ugyanakkor, hogy az Amerikai Egyesült Államokban is megjelenik a *privacy* és az emberi méltóság összekapcsolása. Dean Prosser 1960-as években sokat idézett munkáját felidézve Bloustein vitatkozik azzal, hogy a privacyt érintő jogsértéseket csupán négy, „hagyományos" vétkességi felelősségi formulával lehet leírni (az érintett személyt elvonultságában zavarják, magánszférájába beavatkoznak; az érintettre vonatkozó kellemetlen tények nyilvánosságra hozatala; az érintett nyilvánosság előtt rossz megvilágításba helyezése; az érintett nevével, hasonlóságával való visszaélés – ma úgy mondanánk, személyiséglopás). Bloustein szerint a privacy jogával szembeni jogsértések minden esetben a személyiség ellen irányulnak, támadás az emberi méltóság *(human dignity)* ellen.[1]

Az egyén méltóságának védelme teszi szükségessé és indokolttá az adatok oltalmát a jogellenes hozzáféréssel és felhasználással szemben. Majtényi László hangsúlyozza, hogy a személyes adat védelme az egyén védelmét szolgálja, aki része szűkebb és tágabb közösségének, bonyolult és összetett viszonyok alanya.[2]

Jóri András szerint „az adatvédelmi jog célja a magánszféra védelme".[3] A magánszféra, valamint a személyes adatok védelme az Alaptörvényben

[1] Edward J. Bloustein: Privacy as an Aspect of Human Dignity – An Answer to Dean Prosser. In Ferdinand D. Shoeman (szerk.): *Philosophical Dimension of Privacy – an Anthology*. Cambridge University Press, 1984. 156–202.

[2] Majtényi László így fogalmaz: „Az adatvédelem a személy, az ember, más szóval: az adatalany védelmét, nem pedig magának az adatnak a védelmét jelenti." Majtényi László: *Az információs szabadságjogok – Adatvédelem és a közérdekű adatok nyilvánossága*. Budapest, Complex Kiadó, 2006. 63.

[3] Jóri András: *Adatvédelmi kézikönyv*. Budapest, Osiris Kiadó, 2005. 11.

rögzített,[4] ilyen módon a legmagasabb szintű hazai jogforrási hivatkozást nyújtja, amelyet kiegészítenek a nemzetközi dokumentumok. A magyar adatvédelmi törvény, az információs önrendelkezési jogról és az információszabadságról szóló 2011. évi CXII. törvény (Infotv.) a magánszféra védelmét határozza meg értelmezési keretként, olyan célként, amelyre tekintettel az adatvédelemmel összefüggő jogi kérdések interpretálandók.

Ha az Európai Unió adatvédelmi szabályozására tekintünk, az értelmezési keret középpontjában ott is az alapvető jogok védelme áll. Az 1995-ös adatvédelmi irányelv[5] még nem hivatkozhatott az Európai Unió Alapjogi chartájára,[6] mindazonáltal a jogalkotás mögött ott húzódott a tagállamok alapjogi hagyománya[7] és gyakorlata, valamint az Európai Unió Bíróságának gyakorlata is.

A megjelölt értelmezési tartományok nyújtanak keretet ahhoz, hogy a jogszabályok alkalmazása során a jogalkalmazó megfelelő eredményre jusson, így az egyes jogkérdések megválaszolhatók legyenek. Az egyén számára a jogszabályokban biztosított jogokhoz a kikényszerítés eljárásai és intézményei társulnak.

Az adatkezelő szervezetén belül az adatvédelmi tisztviselőhöz, azon kívül az adatvédelmi hatósághoz, a tagállami rendszerben utolsó jogorvoslati lehetőségként pedig a bírósághoz lehet fordulni. Az egyéni jogok kikényszerítésének európai szintű fórumai az Emberi Jogok Európai Bírósága, valamint az Európai Unió Bírósága. A tagállami szinten meg nem oldott jogviták e fórumok előtt folytathatók, illetve kezdeményezhető az EU jogának értelmezésére irányuló eljárás. Ezek a jogviták az elmúlt évek tapasztalatai szerint hatékony módon járultak hozzá egyes kérdések megválaszolásához.

[4] A magán- és családi élet, valamint a személyes adatok védelméhez fűződő jogot az Alaptörvény VI. cikke rögzíti.

[5] Az Európai Parlament és a Tanács 95/46/EK irányelve (1995. október 24.) a személyes adatok feldolgozása vonatkozásában az egyének védelméről és az ilyen adatok szabad áramlásáról.

[6] Az Európai Unió *Alapjogi chartáját* 2000. december 7-én írták alá Nizzában, azonban csak 2009. december 1-jétől elsődleges jogforrás, és mint ilyen közvetlenül hatályos minden uniós tagállamban.

[7] Lásd bővebben például Belgium tekintetében: Paul De Hert: Belgium, Courts, Privacy and Data Protection: An Inventory of Belgian Case Law From the Pre-GDPR Regime (1995–2015). *Brussels Privacy Hubworking Paper,* 15. (2019), 5.

Az Európai Unió 2016 tavaszán új adatvédelmi tárgyú jogalkotási aktusokat fogadott el:

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 irányelv hatályon kívül helyezéséről (a továbbiakban Rendelet).

Sem a Rendelet, sem a bűnügyi irányelv nem hivatkozik a magánéletre mint a jogi aktus értelmezési keretére, csupán az Alapjogi chartában rögzített jogokra. A jogalkotó ezen a ponton nem adott jogalkotást orientáló értelmezési keretet. A preambulumbekezdésekben értelemszerűen a magánélet védelmének számos aspektusa felmerül, mindazonáltal a korábbi jogi aktussal összevetve ez a különbség szembeötlő.

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

Az úgynevezett e-Privacy irányelvet (2002/58/EK) a jövőben felváltó e-Privacy rendelet is az adatvédelmi szabályozási csomag részét képezi, de lényegesen később alkotják csak meg. Az e-Privacy rendelet jelenleg is csak a tervezet szintjén áll, és már ezt a tervezetet is többször módosították. Az Európai Unió intézményeinek adatvédelmi szabályait, illetve ennek felügyeletét szabályozó 45/2001/EK számú rendelet felülvizsgálata 2018-ban lezárult, helyébe az Európai Parlament és a Tanács (EU) 2018/1725 rendelete (2018. október 23.) lépett a természetes személyeknek a személyes adatok uniós intézmények, szervek, hivatalok és ügynökségek általi kezelése tekintetében való védelméről és az ilyen adatok szabad áramlásáról, valamint a 45/2001/EK rendelet és az 1247/2002/EK határozat hatályon kívül helyezéséről.

Elemzésem az elsőként említett uniós jogalkotási aktusra, az általános adatvédelmi rendeletre (angolul: General Data Protection Regulation, GDPR) koncentrál. A jogi aktus 2018. május 25-től alkalmazandó az Európai Gazdasági Térség tagállamaiban.

Az alábbiakban a Rendeletet és a Rendelet nyújtotta védelem szintjét elemzem.

A védelem szükségességéről

A személyes adatok kezelése egyre nagyobb mértékben befolyásolja az egyének életét. Ez számos jogviszonyban nyilvánvalóvá vált az elmúlt évtizedekben, ahogyan a való élet jelenségei egyre inkább digitálisan is megjeleníthetővé válnak, és az interneten keresztül befolyásolhatók valós körülmények, amelyekre hatásunk korábban csak az offline világban lehetett. Mindemellett az is megfigyelhető, hogy az internetes közeg már nem csupán a való élet leképeződése, kiegészítése, hanem egyre nagyobb szerepet játszanak az online közegben végbemenő események az emberek életében. A való és az online lét közötti kettősségről ír Csepeli György tanulmányában.[8] Az online világ történései már önmagukban is fontos társadalmi események. Mindezeknek a fényében szükséges értékelnie a jogi gondolkodásnak, hogy milyen eszközei vannak a védelem megteremtésére és erősítésére azon adatok tekintetében, amelyek mindezeket a lehetőségeket megteremtik, és amelyek kezelése életeket, élethelyzeteket, emberi kapcsolatokat képes befolyásolni. Az Európai Unió válasza ebben a tekintetben egyértelmű: „ami jogellenes offline, annak online is jogellenesnek kell lennie".[9]

A kockázatokkal és a rosszhiszemű magatartásokkal folyamatosan számolni kell, a védelem végső soron ezekkel szemben fogalmazódik meg.

A Rendelet alkalmazásával egy olyan szabályozás lép világszerte reflektorfénybe, amely a személyes adatok magas szintű védelmét tűzi ki célul. A magas védelmi szint megteremtésében a Rendelet nem egyedül a szabályozásra támaszkodik, hanem több ponton a jogalkalmazóra bízza a jogi megfelelés helyes módjának megtalálását. A korábbi szabályozáshoz képest

[8] Csepeli György: Veszélyesen élni? Avagy az internethasználat kockázatai. In Talyigás Judit (szerk.): *Az internet a kockázatok és mellékhatások tekintetében*. Budapest, Scolar Kiadó, 2010. 25–42.

[9] A Bizottság közleménye az Európai Parlamentnek, a Tanácsnak, az Európai Gazdasági és Szociális Bizottságnak és a Régiók Bizottságának: *Európa digitális jövőjének megtervezése*, Brüsszel, COM(2020)67 végleges, 11. (2020. február 19.)

eltolódik a felelősség az adatvédelmi hatóságoktól az adatkezelők irányába.[10] A szabályozásnak természetesen velejárója marad a kikényszerítés eszközrendszere, de ez is összetettebbé válik a korábbiakhoz képest. Egységes gazdasági térben kívánja az uniós jogalkotó a védelmi szintet fenntartani, illetve megteremteni; a megerősített hatóságokat uniószerte azonos és nagyon erős vizsgálati, korrekciós hatáskörökkel ruházta fel; a Rendeletben meghatározott adatkezelőket arra kötelezi, hogy adatvédelmi tisztviselőt alkalmazzanak a megfelelés érdekében.

Az elmúlt évek bővelkedtek olyan eseményekben, amelyek az adatokkal végezhető jogsértésekről, manipulációkról alkotott elképzeléseinket többször is átalakították.[11] A közösségi oldalak piacáról kiderült, hogy már messze nemcsak közösségi oldalak, hanem jóval többet jelentenek annál. Az életviszonyokat befolyásolni képes gépezetté nőtték ki magukat. Erről írnak részletesen Brendan van Alsenoy és szerzőtársai.[12] A nyitott társadalmú demokráciák azzal szembesülnek, hogy választóik magatartása a róluk kialakított profilok alapján befolyásolhatóvá válik, a választási csalások új dimenzióját nyitva meg.[13] Mindeközben a felhasználók a különböző nemzetbiztonsági szolgálatok hozzáféréseivel kapcsolatos hírek, így az Edward Snowden nevéhez fűződő kiszivárogtatások[14] miatt feladják a magánszféra illúzióját. Az illúziók felszámolásához vezet a globális adatkezelések jelensége is. Az internet teljesen fellazította a korábbi fizikai határokat, a felhasználók körében a védtelenség érzete megerősödött.

A *big data* jelensége a hétköznapi szókincsünk részévé válik, jelezve, hogy mindenkit érint a korábban elképzelhetetlen mennyiségű adatok gyűjtése, elemzése. Újdonságát részben az adja, hogy a korábbi, kisebb minta-

[10] Vö. Maria Eduarda Gonçalves: The EU Data Protection Reform and the Challenges of Big Data: Remaining Uncertainties and Ways Forward. *Information & Communications Technology Law,* 26. (2017), 2. 90–115.

[11] Vö. Tal Zarsky: Privacy and Manipulation in the Digital Age. *Theoretical Inquiries in Law,* 20. (2019), 1. 157.

[12] Brendan van Alsenoy et al.: From Social Media Service to Advertising Network. A Critical Analysis of Facebook's Revised Policies and Terms. *Researchgate.net,* 2015. augusztus 25.

[13] Az Európai Adatvédelmi Biztos 2018. március 19-én nyilvánosságra hozott, 3/2018. számú, *EDPS Opinion on Online Manipulation and Personal Data* című véleménye 13. számú lábjegyzetében utal több forrásra is, amelyek a választások manipulálhatóságának bizonyítékául szolgálnak.

[14] A társadalmi hasznosság és a jogellenesség jelenségét elemzi írásában többek között David E. Pozen. David E. Pozen: *Edward Snowden. National Security Whistleblowing, and Civil Disobedience.* New York, Columbia Law School, 2019.

vételű adatfelhasználásokhoz képest eddig elképzelhetetlen eredményekre lehet jutni.[15] Bár a big data kapcsán nehéz egységes definíciót találni, Ződi Zsolt szemléletesen fogalmazza meg: a jelenség lényege, hogy a külvilág és az emberek egyre több adatát rögzítik, és ezekre az adathalmazokra egyre többféle elemző, profilírozó, következtető és jósló algoritmus épül.[16] A big data nem csupán a piaci szereplők számára érhető el, és kínál előnyöket, hanem, ahogyan Szőke Gergely hangsúlyozza, a közhatalmi szervek is számos területen aknázhatják ki az új lehetőségeket. Így például a közlekedési és szállítási adatok elemzése, az egészségügyi szolgáltatások fejlesztése, az adócsalás és a korrupció elleni küzdelem, a bűnmegelőzés és a büntetőeljárások, vagy akár a munkanélküliség elleni küzdelem, az oktatás és a környezeti adatok elemzése terén is igénybe vehetők a big data elemzések eredményei.[17] Orla Lynskey az adatok koncentrációját és a kapcsolódó hatalmi helyzetet elemezve mutat rá az „adathatalom" jelenségére, amelynek privacyszempontból is különös figyelmet kell szentelni.[18]

Lynskey írásában arra is rámutat, hogy az adatok koncentrációjával járó piaci átrendeződés versenyjogi eszközökkel is kezelhető részben, de a Facebook és a WhatsApp fúziója során az Európai Bizottság nem érvényesítette megfelelően a fogyasztók érdekeit. A hatékony érdekérvényesítéshez három lehetséges utat javasol: erősebb adatvédelmi kikényszerítést, vagy az adatok közjószágként, illetve a technológiai óriások közszolgáltatóként való kezelését, végül pedig a mesterséges adatkoncentráció (Lynskey szóhasználatával: adatkapitalizmus) korlátozását.

Tal Zarsky a Rendelet és a big data között kibékíthetetlen ellentétet lát, ugyanis az adatvédelmi alapelvek a big data alapvető célkitűzéseivel össze-

[15] Lásd ebben a tekintetben: Kenneth Cukier – Viktor Mayer-Schoenberger: The Rise of Big Data – How It's Changing the Way We Think About the World. *Foreign Affairs,* 92. (2013), 3. 28–40.

[16] Vö. Ződi Zsolt: Privacy és a Big Data. *Fundamentum,* 21. (2017), 1–2. 18.

[17] Szőke Gergely László: Big Data and Algorithms in the Public Sector and Their Impact on the Transparency of Decision-making. In *Central and Eastern European e|Dem and e|Gov Days 2018*. Viena Austrian Computer Society, 2018. 301–311.

[18] Vö. Orla Lynskey: Grappling with "Data Power": Normative Nudges from Data Protection and Privacy. *Theoretical Inquiries in Law,* 20. (2019), 1. 189–220.

egyeztethetetlenek.[19] Négy példát is említ erre: a célhozkötöttség elvét, az adatminimalizálást, a különleges adatok kezelésére vonatkozó korlátozásokat és az automatikus egyedi döntéseket.

A mesterséges intelligencia térnyerése egy másik jelenség, amelyet ezekben az években próbálunk megismerni és megérteni. Nem csupán a technológiát, hanem annak alkalmazását és az emberek életére gyakorolt hatását is kutatjuk, Hajdú József például a munkaerőpiaci hatásait.[20]

> Hajdú nemzetközi kitekintés keretében elemzi a munkaerőpiaci hatásokat, rámutatva arra, hogy egyes szektorokban kisebb, míg másokban nagyobb eséllyel váltják fel robotok az embereket. Bár itt a munkaerőpiaci hatásokról van szó, a mesterséges intelligencia mindig szorosan kapcsolódik személyes adatok felhasználásához, így a munkahelyi környezetben szintén érzékenynek számít ez a kérdéskör.

Kollár Csaba arra mutat rá, hogy a mesterséges intelligencia jellegzetesen interdiszciplináris terület, amelynek számos alfaja ismert. A témában kiváló alapvetésnek is tekinthető írásban Kollár a biztonságtudomány, a számítástudomány, a kommunikáció- és nyelvtudomány, a pszichológia, a szociológia, a filozófia, a matematika és informatika, a műszaki tudományok, az idegtudomány, valamint a biológia és az orvostudomány által is támogatott jelenségként, technológiaként írja le a mesterséges intelligenciát. A mesterséges intelligencia legfontosabb alfajai között a gépi tanulást, a természetes nyelv feldolgozását, a szakértői rendszereket, a látást, a beszédet, a tervezést és a robotikát említi.[21]

Még akkor is, ha egyre többet meg tudunk érteni az új technológiából, az alkalmazói nem mindig tesznek sokat a transzparencia érdekében.

Az innováció és az adatvédelem közötti konfliktust divatos említeni. E kettő kibékítésére tesz kísérletet például Sophie Stalla-Bourdillon és Alison Knight, akik nem vitatják a magánszférát érintő kihívásokat,

[19] Vö. Tal Zarsky: Incompatible: The GDPR in the Age of Big Data. *Seton Hall Law Review,* 47. (2017), 4(2). 995–1020.

[20] Vö. Hajdú József: Az innováció hatása a munkaerőpiacra, avagy elveszik-e a robotok az ember munkáját? *Forum: Acta Juridica et Politica,* 10. (2020), 2. 37–55.

[21] Kollár Csaba: A mesterséges intelligencia kapcsolata a humán biztonsággal. *Nemzetbiztonsági Szemle,* 6. (2018), 1. 5–23.

de az emberi beavatkozás és a felügyelet szükségességét hangsúlyozzák.[22] Nicholas Diakopoulos szintén az átláthatóság mellett érvel, és az egyébként a magánszféra védelmére is használható algoritmusok kapcsán a rajtuk keresztül használt hatalom tisztázását szorgalmazza.[23] Eszteri Dániel a mesterséges intelligencia és a GDPR elemzése kapcsán kiemeli az emberi beavatkozás szükségességét, a tisztességes adatkezelés követelményeit.[24] Az adatvédelem eddig ismert fogalom- és szabályrendszerének kereteit minden bizonnyal feszegetni fogja a mesterséges intelligencia számos alkalmazása. Eszteri Raymond Kurzweilt idézi, aki szerint a technológiai fejlődés eléri a szingularitás jövőbeli korszakát, amelyben „a technológiai változás üteme olyan gyors lesz, a hatása pedig oly mély, hogy az emberi élet visszafordíthatatlanul átalakul".[25] Ennek hatásai a magánszféra- és az adatvédelemben is folyamatos kutatások tárgyát kell hogy képezzék.

A személyi és szervezeti informatikai igényeket egyre nagyobb mértékben felhőszolgáltatások révén szolgálják ki. Ez a tendencia – amely mellett adatbiztonsági, adatvédelmi megfontolások is felsorakoztathatók – szükségszerűen váltja ki a jogi szabályozás nélkülözhetetlenségéről szóló gondolkodást.[26] Az informatikai megoldások a folyamatosan bővülő igényekhez dinamikusan alkalmazkodnak, amelyek újabb és újabb kérdéseket vetnek fel a technológia és az adatvédelem határán.[27]

[22] Sophie Stalla-Bourdillon – Alison Knight: Data Analytics and the GDPR: Friends or Foes? A Call for a Dynamic Approach to Data Protection Law. In R. Leenes – R. van Brakel – S. Gutwirth – Paul De Hert (szerk.): *Data Protection and Privacy: The Internet of Bodies Hart*. Oxford, Hart Publishing, 2018. 317–328.

[23] Nicholas Diakopoulos: *Algorithmic Accountability Reporting: on the Investigation of Black Boxes.* Colombia Journalism School – Tow Center for Digital Journalism, 2013.

[24] Eszteri Dániel: Hogyan tanítsuk jogszerűen a mesterséges intelligenciánkat? *Magyar Jog,* 66. (2019), 12. 669–682.

[25] Eszteri (2019): i. m. 671.

[26] A felhőszolgáltatásokra vonatkozó jogi szabályozás szükségességéről vö. Váradi Szilvia – Kertész Attila – Michael Parkin: The Necessity of Legally Compliant Data Management in European Cloud Architectures. *Computer Law & Security Review,* 28. (2012), 5. 577–586.

[27] A legújabb ködrendszerekre vonatkozó adatvédelmi szabályokról lásd bővebben: Gizem Gültekin Várkonyi – Váradi Szilvia – Kertész Attila: Legal Aspects of Operating IoT Applications in the Fog. In Buyya Rajkumar – Narayana Srirama Satish (szerk.): *Fog and Edge Computing: Principles and Paradigms*. Hoboken, John Wiley & Sons, 2019. 411–432.

A végleges formáját 2020-ban elnyerő kínai társadalmi pontrendszer minden bizonnyal nem csupán egyetlen ország belügye marad.[28] Félő, hogy ennek hatása meg fog jelenni Európában is.

Az említett példák jól illusztrálják a technológia jelentette kihívásokat. A sort hosszan lehetne folytatni, itt leginkább csak a látványos, az irodalomban részletesen feldolgozott technológiákra tértünk ki.

Hogyan hat mindez a magánszférára? A magánszféra állapotát illetően eltérhetnek az álláspontok, mindazonáltal a szabályozással szembeni elvárások nagyon magasak, különös tekintettel a gyorsan változó technológiai környezetre. Az adatok védelmét illetően gyakran nem annak szintje, hanem egyáltalán a létezése kérdés. Van-e még védelem – elsősorban az online közegben – a magánszférát illetően?

A következő években dől el, hogy miként állja majd ki a Rendelet az idő próbáját, mennyiben minősül helyes jogalkotói válasznak a gyakorlati kihívások tükrében. Nem csupán Európában, hanem szerte a világon nagy figyelem övezi az új szabályozás gyakorlati alkalmazását, sikere vagy sikertelensége hatással lesz más kontinensek szabályozására, illetve értelemszerűen az Európai Unió által biztosított védelem minőségére is. Ennek azért is van jelentősége, mert, ahogy az Európai Bizottság közleménye is rámutat: a „világ több országa is sok esetben az EU erős adatvédelmi rendszeréhez igazította saját jogszabályait".[29]

Azt látjuk tehát, hogy a személyes adatok felhasználásának és védelmének szabályozása a 21. század elején meglehetősen nagy jelentőséggel bír, és a személyes adatkezelések bővülésével folyamatosan növekedik majd a jelentősége a jövőben is.

A Rendelet az elmúlt években az egyik legnagyobb figyelemmel kísért változást eredményezte az Európai Unió jogában. Az új adatvédelmi rendelet alkalmazásának messzemenő jogi és gyakorlati következményei vannak, elemzésem ennek a védelemnek a definiálására és a lehetséges védelmi szintek összehasonlítására irányul.

[28] Vö. Daithí Mac Síthighand – Mathias Siems: The Chinese Social Credit System: A Model for Other Countries? *EUI Working Papers,* (2019), 1.

[29] A Bizottság közleménye az Európai Parlamentnek, a Tanácsnak, az Európai Gazdasági és Szociális Bizottságnak és a Régiók Bizottságának: *Európa digitális jövőjének megtervezése,* Brüsszel, COM(2020)67 végleges, 15. (2020. február 19.)

Vákát

A védelmi szint kérdéseinek vizsgálata

Elemzésemben arra a kérdésre keresem a választ, hogy a személyes adatok védelmének szintje jogi eszközökkel meghatározható-e, illetve a védelem egyes szintjei definiálhatók-e. Amennyiben igen, úgy melyek azok a kritériumok, amelyek alapján az egyes szintek között minőségi különbség tehető? Mi az egyes szintek közötti összehasonlítás alapja? Mindezek fényében milyen lehetőségek adódnak a védelem szintjének alakítására, milyen jogi eszközökkel javítható a védelem minősége?

Az elemző munka a Rendelet kiválasztott szabályainak megértésére, tartalmuk pontos megállapítására és helyes alkalmazásukra irányul. A cél egy olyan szempontrendszer, a védelmi lépcső elméletének megalapozása, amely a védelem szintjének elemzése során jogi értelemben is megragadható szempontokat nyújt. A kiindulópontot minden esetben a hatályos szabályozás, a jelenlegi szint azonosítása jelenti, amelyet összevetek a megelőző szinttel, és kísérletet teszek az új szint meghatározására. Ez a munkamódszer a gyakorlat számára is hasznos lehet.

Az adatvédelmi ügyek nap mint nap nagy számban merülnek fel a gyakorlat során. Ezek egy része, egy sajátos szűrőn, leginkább érintetti panaszok útján eljut az adatvédelmi hatóságokhoz, majd ezek egy szegmense, ismét egy válogatás eredményeként, az európai uniós fórumokhoz. Legyen szó bármilyen ügyről, ugyanazt a jogi mércét alkalmazzuk, korábban a 95/46/EK irányelvet, 2018 májusától pedig a Rendeletet. Bár végső soron mindig ugyanaz a kiindulópont, nevezetesen az egyének magánszférájának, illetve személyes adatainak védelme, hasznos tudományos igénnyel kidolgozni és áttekintést nyújtó elemzést készíteni arról, hogy miből áll össze az a védelem, amit mindig *adatvédelem*ként említünk. Úgy tűnik, mintha magától értetődő lenne a jelentése, mégsem rajzolódik ki következetesen annak rendszerszerű alapja.

A tömegével előforduló és a nehéz ügyekben egyaránt hasznosítható elemzést kívánok bemutatni. Az elvégzett elemzés nem csupán tudományos megfontolásokat kíván szolgálni, hanem célja az egyes ügyek megértését és értelmezését is elősegíteni, ilyen értelemben a gyakorlatra tekintettel készült. Gyakorlati beállítottságú szerzőként közelítem meg a témát, de a napi hatósági munka során is fel kell ismerni, hogy az elméleti kérdések elmélyült vitatása mindig hozzájárul a gyakorlati munka hatékonyságához. A munka hatékonysága – ideértve a hatósági munka hatékonyságát

is – jelentős kérdés a hatóságok által betöltött demokratikus szerep érvényesülésében és értékelésében. Erre a hatóságokról szóló fejezetben bővebben is ki fogok térni.

Módszertani, értelmezési és rendszertani kérdések

A kutatás során a klasszikus kutatási módszerekre támaszkodtam. Szembesültem olyan rendszertani kérdésekkel is, amelyek az elemzés összefüggéseinek összetett voltára, egyszersmind az adatvédelem mint viszonylag fiatal jogterület helykeresésére is utalnak.

A kutatás módszere

A kritikai, forráselemző módszert követtem a vonatkozó szakirodalom feldolgozása terén. A védelmi lépcső elméletének kidolgozása és megalapozása során alkalmaztam az összehasonlító és a történeti módszert is.

A kívánatos védelmi szint meghatározása során értelemszerűen a jogfejlesztésre irányuló javaslatokat fogalmazok meg, ennek kapcsán pedig a *de lege ferenda* megközelítést alkalmazom. A jelenlegi védelmi szint meghatározása során pedig a deskriptív, illetve ehhez szorosan kapcsolódva a kritikai-elemző módszert használom.

A nyelvtani értelmezés

A nyelvtani módszer a normaszöveg pontos tartalmának feltárására irányul. Az Európai Unió jogalkotásának sajátosságaira tekintettel bizonyos esetekben a jogalkotás eredeti, angol verziójának vizsgálata is szükséges. A Rendelet, az Európai Unió valamennyi jogalkotási aktusához hasonlóan, az EU mind a 24 hivatalos nyelvén nyilvánosságra kerül.[30] Értelemszerűen a magyar nyelvi verziót veszem alapul, mint az Európai Unió egyik hivatalos nyelvén, a Hivatalos Közlönyben publikált szöveget.

Az adatvédelmi jog terminológiája nemzetközi téren kidolgozott és mára több évtizedes joggyakorlat után megszilárdult. A normaszöveg köznyelvi

[30] Az Európai Unió hivatalos lapjának honlapja. *Eur-lex.europa.eu*.

alapú értelmezésének alapja a Rendelet számos fogalommeghatározása, amely a köznyelvitől eltérő jelentés szaknyelvi tisztázását segíti elő.

A normacél szerinti (teleologikus) értelmezés

Az Európai Unió jogalkotási rendje szerint a normaszöveget megelőzi a jogalkotói megfontolásokat, célokat összegző preambulumbekezdések sora. A Rendelet 173 ilyet tartalmaz. Az értekezésben a preambulumbekezdéseket a jogalkotói cél tekintetében részletesen elemzem.

A preambulumbekezdéseken túl az adatvédelmi alapelvek absztrakt módon fogalmazzák meg a jogalkotó célját. Az alapelveket az elemzés során figyelembe kell venni a jogalkotói szándék tekintetében.

Az Európa-konform jogértelmezés

Triviálisnak tűnhet, hogy az Európai Unió Rendeletét Európa-konform jogértelmezési módszerrel kell vizsgálni, azonban a joggyakorlat rámutat ennek szükségességére. Az egyes jogkérdéseknek az Európai Unió Bíróságának döntéseiben megjelenő értelmezései a Rendeletbe már részben beépültek, részben pedig magának a Rendeletnek az értelmezését segítik elő. Az Európai Unió Bíróságának immáron számos ítélete született előzetes döntéshozatali eljárás során, és fontos jogértelmezési kérdésekben nyújt eligazítást nem csupán a kérdéseket előterjesztő bíróságoknak, hanem a hatóságoknak és a többi jogalkalmazónak egyaránt. Tekintettel a nem mindig koherens tagállami jogalkalmazásra, az Európa-konform módszer fontos a Rendelet helyes értelmezésének feltárásában. A teljes harmonizáció jogalkotói célkitűzése áthatja a Rendelet szabályait, ennek a norma értelmezésére és alkalmazására is kihatással kell lennie.

A Bodil Lindqvist-ügyben hozott ítéletében az Európai Unió Bírósága már az adatvédelmi irányelv értelmezését illetően is a teljes harmonizációt tartotta szem előtt. A 2003. november 6-án kelt ítélet 96. pontja szerint: „Az említett nemzeti jogszabályok harmonizációja tehát nem korlátozódik minimális mértékű harmonizációra, hanem annak lényegében teljes harmonizációt kell eredményeznie. E szemlélet alapján a 95/46 irányelv célja a személyes adatok

szabad áramlásának biztosítása, garantálva az ezen adatokkal érintett személy jogai és érdekei védelmének magas szintjét."[31]

Rendszertani kérdések

A Rendelet egyik sajátosságát kutatási szempontból az adja, hogy a jogágak tekintetében nem világos az elhelyezkedése. Közjogi jellege egyértelmű akkor például, amikor az adatvédelmi felügyeleti hatóság feladat- és hatáskörét határozza meg, mindazonáltal az adatkezelő és az adatalany viszonylatában egymásnak mellérendelt felek jogait és kötelezettségeit is rendezi, sok esetben diszpozitív módon. A jogvédelem vertikális és horizontális dimenzióját is biztosítani hivatott a Rendelet. Ennek megfelelően mind a közjogi, mind a magánjogi jogágba beletartozik. A normák általános kógenciája mellett a magánjogi jellege is meghatározó.

A személyes adatok védelméhez fűződő jog elsősorban az állami szereplőkkel szemben fogalmazódott meg (közjogi jelleg), majd az adatkezelések tömegessé válásával ez a jelleg megszűnt (magánjogi jelleg). Nemcsak az adott időpontban hatályos jogi szabályozás tekintetében, hanem a jogfejlődés történetiségében is megragadhatók a rendszertani kérdések.

Rendszertani elhelyezkedésének bizonytalanságai a Rendelet szabályainak megértését, a norma tartalmának pontos megállapítását nem hátráltatják ugyan, mégis vezethetnek olyan jogértelmezési kérdésekhez, amelyekben e kettősség szem előtt tartása hozzásegíthet a helyes megoldás megtalálásához.

[31] C-101/01. sz., a Bodil Lindqvist kontra Svédország ügyben 2003. november 6-án hozott ítélet.

A védendő jog és a védelem szintjének kérdései a személyes adatok vonatkozásában

A bevezetőben utaltam a magánszférához fűződő jogra, amelyet értelmezési keretként használunk a személyes adatok védelméhez fűződő jogi kérdések megválaszolása során.

> A magánszféra, a magánélet és az angolszász irodalomban használatos privacy jelentéstartalma rokon, de nem azonos. Nem célom e három fogalom összehasonlítása, mindenesetre a fogalmakat a személyes adatok védelme szempontjából hasonlóan fontosnak tekintem, egymás szinonimáiként kezelem és említem. Hijmans is utal téziseiben a magánélet és az adatvédelem, illetve privacy különbözőségeire. Az EEJE 8. cikkében rögzített magánélet magában foglal olyan, az adatvédelmen túlmutató aspektusokat is, mint az otthon és a levéltitok, a családi élet védelme.[32]

A fogalmi kérdéseket nem kívánom a szükségesnél részletesebben tárgyalni. Külön kötet tárgyát képezhetné, ha a témát részletesen ki szeretnénk dolgozni. Ennek megfelelően csak egy áttekintést adok a védendő jogról annak érdekében, hogy a későbbi fejezetek alapjául és hátteréül szolgáljon.

A magánszféra fogalmának születése: a magánszféra és a technológia összefüggései

Ha történetileg a magánszféra igényének, majd jogának megjelenése elé tekintünk, akkor a technológiai fejlődés által ösztönzött jogfejlődést kell felidéznünk. Székely Iván már a telefonok megjelenését egy olyan „omlásnak" tekinti a magánszféra védelmében, amely a 19. század második felében megváltoztatta a magánszféra határait, és a „telefonkészülék egyik fő eleme, a mikrofon önálló karriert kezdett, és ezzel kialakult a vezetékes

[32] Hielke Hijmans: *The European Union as a Constitutional Guardian of Internet Privacy and Data Protection*. PhD-értekezés. Amszterdam, University of Amsterdam, 2016.

»poloskák« első generációja".[33] A 19. század végén a gyors exponálású fényképezőgépek megjelenésével[34] addig nem tapasztalt gyorsasággal és módon vált megjeleníthetővé az ember képmása. (A Kodak 1888-ban dobta piacra azt a fényképezőgépét, amellyel gyakorlatilag amatőrök is képesek voltak jó minőségű képeket készíteni.) Lehetőség nyílt arra, hogy bárkit bárhol lefényképezzenek, majd azt az újságokban közzétegyék. Erre a jelenségre válaszul fogalmazódott meg Louis D. Warren és Samuel D. Brandeis írásában a modern kori ember vágya, hogy egyedül, illetve békén hagyják.[35] A magánszféra-védelem jogtörténeti előzménye ez a vágy, amely aztán az egyedülléthez (másoktól való zavartalansághoz) való jogként *(the right to be let alone),* vagy megint másként, a privacy jogaként fogalmazódott meg.

A privacy fogalmának történeti fejlődését vizsgálva rossz példaként szokás felhozni Jeremy Bentham tervét a börtönben fogva tartottak megfigyelésére.[36] A büntetőjoggal magas szinten foglalkozó Bentham kiindulópontja gyakorlatilag az volt, hogy miként lehet a börtönt hatékonyan berendezni, és a lehető legnagyobb fegyelmet, biztonságot megteremteni. (Nem csupán börtön, hanem más célú épületekre is alkalmazhatónak tartotta a panoptikon gondolatát, így többek között dologházakra, kórházakra, tébolydákra, de még szegényházakra vagy akár iskolákra is.) Olyan börtön tervét alkotta meg, amelyben a fogvatartottak egy központi toronyból, a kör alakú épület közepén elhelyezkedő pozícióból bármikor megfigyelhetők. Fizikailag természetesen képtelenség, hogy az őr valamennyi fogvatartottat egyszerre megfigyelje, a fogvatartottban mégis azt az érzést kelti a megfigyelés lehetősége, hogy valóban megfigyelik, és ezért magatartását ennek megfelelően alakítja. A görög szóból eredő, a „mindent látó" megoldás révén ez a társadalmilag is jelentős elképzelés a *panoptikon* nevet viseli. A privacygondolkodásban ez a koncepció széles körben hivatkozott, hiszen nem csupán egy épületre, hanem egy szélesebb közösségre is alkalmazható a panoptikon jelensége és az emberi kapcsolatokra, emberi magatartásra való hatása.[37]

[33] Székely Iván: Kukkoló társadalom – avagy van-e még függöny virtuális ablakunkon. In Talyigás Judit (szerk.): *Az internet a kockázatok és mellékhatások tekintetében*. Budapest, Scolar Kiadó, 2010. 93–20.

[34] Original Kodak Camera, Serial No. 540. *Americanhistory.si.edu.*

[35] Louis D. Brandeis – Samuel D. Warren: The Right to Privacy. *Harvard Law Review,* 4. (1890), 5. 193–220.

[36] Jeremy Bentham: *Panopticon or the Inspection-House.* (h. n.), (k. n.), 1787.

[37] A panoptikon gondolatáról és az egyénekre gyakorolt lélektani hatásáról értekezik Michel Foucault: *Discipline and Punish – The Birth of the Prison*. New York, Pantheon, 1977.

Bentham börtöntervének van egy olyan aspektusa is, amely kevesebb figyelmet kap. Ez pedig magának a börtönőrnek a megfigyelésére irányul. Elgondolásának része volt ugyanis, hogy a megfigyeléssel megbízott börtönőrt is meg kell figyelni, mégpedig nem csupán a felettesei révén, hanem bárki által, a *köz* által. Függetlenül attól, hogy a 18. század végén alkotó szocialista gondolkodó Benthamet ezen a ponton egyfajta naivitással is lehet vádolni, a privacy kapcsán egy fontos hivatkozási pontként jelenik meg a demokratikus kontroll szerepe. A panoptikon gondolata az elszámoltathatóság követelményével társulva már jóval közelebb áll a modern kori privacygondolkodáshoz. Nem abban az értelemben természetesen, hogy a panoptikonelgondolás legitim lenne, hanem olyan megvilágításban, hogy az információk kezelőinek hatalmi pozícióját erős felügyelettel, és ahol lehet, közösségi ellenőrzést lehetővé tevő transzparenciával kell kiegészíteni.

A 20. század második felében a jogi gondolkodást a számítógépek megjelenése és széles körű felhasználásával kapcsolatos aggályok határozták meg. Alan J. Westin már az 1960-as évek fejleményeit elemezve arra jut, hogy a technológia fejlődése látványos ugyan, de „halljuk a riasztó hangját is a privacy jövőjét illetően a számítógépes adatbankok korában", a személyes találkozásokat felváltó időszak „elembertelenedése", és a demokratikus felhatalmazás nélküli „technológiai elitek lehetséges megjelenése" miatt. A fél évszázaddal ezelőtti, Westintől származó gondolatok akár prófétainak is tekinthetők, mindazonáltal rámutatnak arra, hogy a technológia és a privacy metszéspontjában évtizedek óta hasonló problémák merülnek fel.[38]

A magánszférát érintő negatív elképzelések között kortársainktól származó idézetek is felhozhatók. Legyen elég itt csupán két megnyilvánulásra utalni. A Google vezérigazgatója, Eric Schmidt egy CNBC-interjúban arra a kérdésre, hogy a felhasználók szabadon megoszthatnak-e információkat a Google-lal, mint egy bizalmas baráttal, a válasza az volt, hogy „ha nem szeretnél valamit megosztani mással, akkor először is talán nem kellene megtenned".[39] Felmerül a kérdés, hogy a világ legnagyobb keresőmotorjának vezetőitől a privacy iránt nagyobb fogékonyságot várnának-e el a felhasználók.

[38] Alan F. Westin (szerk.): *Information Technology in a Democracy*. Cambridge, Massachusetts, Harvard University Press, 1971.

[39] A CNBC-nek 2009. december 3-án adott interjújában hangzott el a hírhedtté vált mondat: „If you have something that you don't want anyone to know, maybe you shouldn't be doing it in the first place." Forrás: Electronic Frontier Foundation honlapja.

A másik idézet Mark Zuckerbergtől, a Facebook alapítójától származik, akinek azt a kijelentést tulajdonítják, hogy a *privacy már nem társadalmi norma*. Függetlenül attól, hogy az idézet nem szó szerinti, a 2010-es nyilatkozat óta a szavak és a tettek közötti összhangot illető valamennyi kétségünk eloszlatására elegendő érvet kaptunk.[40] Egy Európai Unió szintű 2019-es közvélemény-kutatás szerint a megkérdezetteknek csak egyötöde osztja teljes mértékben ezt a megközelítést.[41] Érdekességképpen: a 2010-ben készített kutatás egy kissé eltérő attitűdről tanúskodik, akkor még a válaszadók 33%-a nyilatkozott úgy, hogy személyes adatok megosztása „nem nagy dolog".[42]

A magánszférához fűződő igény és a technológia viszonya mindvégig meghatározó a személyes adatok kezeléséről és védelméről folytatott gondolkodás során. Ez így van már a 19. század második fele óta, és magától értetődőnek tűnik, hogy velejárója marad a modern kori emberiségnek. „Minél inkább támaszkodik az ember a modern technológiákra, egyre kiszolgáltatottabbá, sérülékenyebbé válik emberi méltósága, magánszférája."[43] A 20. század végén megfogalmazódott információs önrendelkezési jog jól tapintott rá az egyén kiszolgáltatottsága miatti jogvédelmi űrre. E jog az adat alanyának kívánta visszaadni azt, amit veszély fenyegetett, nevezetesen azt a döntést, hogy mi történjék személyes adataival. Több évtizedes távlatban és a technológia által kínált új lehetőségek közepette csalókának tűnik a kép, hogy az érintett lesz az, aki képes minden élethelyzetben megítélni a magánszféráját érintő hatásokat, majd az optimális döntést meghozni személyes adatai felhasználását illetően. Úgy tűnik, a technológia sokkal több lehetőséget nyújt az adatok rejtett felhasználására nézve, semmint hogy a jogalkotó a magánszférát érintő minden eshetőségre megoldást találhatna – az adatalanyról nem is beszélve. A 21. század elején a védelmi deficit nyilvánvaló. A fentebb leírt jelenségek, mint a big data vagy a mesterséges intelligencia alkalmazásának térnyerése ezt a deficitet tovább szélesíti.

[40] A beszéd 2010 januárjában San Franciscoban hangzott el. *Theguardian.com*.

[41] Special Eurobarometer (487a) Report: The General Data Protection Regulation. *Europa.eu/eurobarometer,* 2019. június, 63–67.

[42] Special Eurobarometer Report (359): Attitudes on Data Protection and Electronic Identity in the European Union. *Europa.eu/eurobarometer,* 2011. 30–32.

[43] Szabó Endre Győző: Méltóság és megfigyelés – Az emberi méltóság: érték és mérce. *Jogi Fórum,* 2009. július 13.

Miben áll a védelmi deficit? Az adatkezelést érintő döntések átláthatatlanok, a döntések előkészítésére a hatóságoknak általában nincs rálátásuk. Az adatok az alkalmazott technológia sajátosságainak megfelelően láthatatlanok az emberi szem számára, az adatokon végzett műveletek szintén láthatatlan módon végrehajthatók, és az érintettek, a hatóságok, de még az adatvédelmi tisztviselő előtt is rejtve maradhatnak. Még akkor is, ha a döntések híre vagy a jogellenes adatkezelés jelei megmutatkoznak, a bizonyítás nem feltétlenül könnyű, a legtöbb esetben speciális szakértelmet igényel. Ez a szakértelem az adatvédelmi felügyeleti hatóságoknál sem mindig áll házon belül rendelkezésre. Ebben a tekintetben Charles Raab és Székely Iván közös tanulmányára később még kitérek, itt csak arra szorítkozom, hogy a tanulmány egyik fontos megállapítása szerint az adatvédelmi hatóságoknál a rendelkezésre álló informatikai és kommunikációs technológiai szakértelem nem kielégítő, vagy legalábbis továbbfejlesztésre szorul.[44] És még abban az esetben is, ha egy bonyolult tényállás napvilágra kerül, az érintett nem feltétlenül tudja érdekeit érvényesíteni, jogait kikényszeríteni adott esetben egy tengerentúli adatkezelővel szemben.

Nem véletlen, hogy ezek a körülmények tükröződnek a közvélemény-kutatásokban is. Az Eurobarometer 2015-ös kutatása szerint az online üzleti szereplők, így a keresőmotorok, közösségi oldalak, e-mail-szolgáltatók esetében csupán a megkérdezettek 3%-a nyilatkozott úgy, hogy teljes mértékben megbízik bennük.[45]

A Rendelet extraterritoriális hatálya a védelmi deficitet ebben a tekintetben csökkentheti, továbbá hozzájárulhat az érintetti jogérvényesítés előmozdításához.[46]

A védelmi deficit másik dimenziója egy folyamatos késztetésként írható le, amely mind az állami, mind az üzleti adatkezelőket érinti. Nevezetesen arról van szó, hogy ami lehetséges technikailag, azt a megfigyelés, vagy éppen üzleti érdekek céljából, vagy egyszerűen kísérletek, kutatások céljából

[44] Charles Raab – Székely Iván: Data Protection Authorities and Information Technology. *Computer Law & Security Review,* 33. (2017), 4. 421–433.

[45] Special Eurobarometer Report (431): Data Protection (Adatvédelem). *Europa.eu/eurobarometer,* 2015, 64.

[46] A Rendelet 3. cikk (2) bekezdése vezeti be az irányultsági szabályt, amelynek révén az ott leírt esetekben az Európai Unión kívüli adatkezelésekre, illetve adatkezelőkre is alkalmazandóvá válik a Rendelet.

meg is teszik. Szabó Máté Dániel az információs hatalom eszközeinek elemzése során a megfigyelés, elrejtőzés és az információs monopólium jelenségét különbözteti meg. Elemzésében az egyén helyzete, az ő kiszolgáltatottsága áll a középpontban. Szabó szerint az „információs értelemben aszimmetrikus viszony hatalmi jellegét az adja, hogy kiszolgáltatottságot hoz létre, mégpedig úgy, hogy az egyént korlátozza cselekvési és döntési szabadságában".[47]

Joshua A. T. Fairfield és Christoph Engel a magánszféra közösségi dimenzióját hangsúlyozzák. Véleményük szerint az egyénre vonatkozó adat egyre kevésbé tekinthető csupán egy személy adatának. Egy adott személy vigyázatlansága saját adataival mások magánszféráját is érinti. Szerintük az „egyéni rendelkezés az adatok fölött egy rossz koncepció", mert képtelenség megbecsülni, hogy milyen eredményekre vezet, ha adatok millióit összekapcsolják és elemzik. A big data korában az információs önrendelkezés tehát illuzórikussá válik.[48] Giovanni Buttarelli korábbi európai adatvédelmi biztos gyakorlatilag ezzel egyező következtetésre jut az online manipuláció vizsgálata körében.[49]

Az adatkezelést érintő újabb és újabb ismereteink megerősítik azt a benyomásunkat, hogy a jog kiszorul az adatkezelések rejtelmes világából, és döntések sora úgy születik meg, mintha a jogállami garanciák következmények nélkül kiiktathatók lennének. Ahogyan Warren és Brandeis az élet minőségére utalt a privacy kapcsán, úgy Westin is azzal érvel, hogy az intenzív intellektuális és érzelmi élet, a civilizációval együtt járó szenzációk hajszolása megmutatta, hogy *az emberi fájdalom, öröm – és profit csak egy része rejlik a fizikai dolgokban*.[50] El kell ismernünk, hogy a privacy illúziójának elvesztése súlyos megállapítás, amely az élet minőségében, a szabadságának élvezhetőségében is deficithez vezet. A technológia megjelenése a hétköznapokban megerősítette a privacy sérülékenységének érzetét, W. H. Ferry

[47] Szabó Máté Dániel: *Az információs hatalom alkotmányos korlátai*. Miskolc, Miskolci Egyetem, 2012. 14.

[48] Joshua A. T. Fairfield – Christoph Engel: Privacy as a Public Good. *Duke Law Journal,* 65. (2015), 3. 385–457.

[49] Repurposing of Data is Likely to Affect a Person's Informational Self-determination. In European Data Protection Supervisor Opinion on Online Manipulation and Personal Data. *Edps.europa.eu,* 2018. március 19.

[50] Alan Westin: The Origins of Modern Claims to Privacy. In Ferdinand D. Shoeman (szerk.): *Philosophical Dimensions of Privacy, An Anthology.* Cambridge University Press, 1984. 76.

egyenesen úgy fogalmaz, hogy „a privacy ma már halott, a technológia ölte meg".[51] Mindez a gyanakvás mérhető „eredményekben" is megmutatkozik, a közvélemény-kutatások megerősítik ezt. Az Eurobarometer felmérése szerint az Európai Unióban tízből legalább hat ember aggódik amiatt, hogy nincs ellenőrzési lehetősége a személyes adatai felett, ötből pedig csupán egy válaszadó érzi úgy, hogy az adatok online gyűjtése során teljes körű tájékoztatást kap az adatkezelés körülményeiről.[52] Az online adatkezelés tehát a felhasználók túlnyomó többségének bizalmatlansága mellett történik.

A 2010-es kutatás[53] eredménye szerint tízből hét uniós polgárt aggaszt, hogy a cégek mit tesznek azokkal az adatokkal, amelyeket ők maguk hoztak nyilvánosságra. Az Eurobarometer 2015-ös elemzése szintén megerősíti ezt az eredményt, ott is pont ilyen arányban, 81%-ban nyilatkoztak úgy a megkérdezettek, hogy csak részlegesen, vagy egyáltalán nem tudják kontrollálni az adataik útját.[54]

Ez a bizalmatlanság akkor, amikor elér egy kritikus mértéket, arra ösztönzi a felhasználókat, hogy a magánszférát erőteljesen védő, gyakorlatilag anonimitást biztosító technológiát alkalmazzanak. Aleecia M. McDonald elemzése szerint ez az ösztönzés csak akkor elégséges, ha valóban közvetlen és erőteljes hatás éri a fogyasztót, vagy a felhasználók közösségét.

McDonald a Duckduckgo keresőmotor, a Tor böngésző, valamint a Pretty Good Privacy (PGP) titkosító kulcs használatát elemzi. Számok alapján kimutatta, hogy a Duckduckgo oldalán végrehajtott keresések és a PGP-felhasználások a Snowden-féle kiszivárogtatások után szignifikánsan megnőttek. A névtelenséget ígérő Tor böngésző Törökországban a politikai tiltakozások közepette

[51] W. H. Ferry: The Need for New Constitutional Controls. In Alan F. Westin (szerk.): *Information Technology in a Democracy*. Cambridge, Massachusetts, Harvard University Press, 2013. 209.

[52] Special Eurobarometer (487a) Report: The General Data Protection Regulation, *Europa.eu/eurobarometer,* 2019. június, 39–43.

[53] Special Eurobarometer Report (359): Attitudes on Data Protection and Electronic Identity in the European Union (Az adatvédelemmel és az elektronikus személyazonossággal kapcsolatos hozzáállás az Európai Unióban). *Data.europa.eu,* 2021.

[54] Special Eurobarometer Report (431): Data Protection (Adatvédelem). *Europa.eu/eurobarometer,* 2015. 9–11.

biztonságos kommunikációt tett lehetővé a tiltakozók számára, és a Tor használata a választások körüli hetekben felfutott.[55]

A bizalmatlanság, úgy tűnik, megfér a kényelmi szempontokkal is. Bruce Schneier szerint épp a kényelmességünk ad lehetőséget arra, hogy felhasználóként megfigyeljenek bennünket. „A vállalatainknak odaadjuk az adatainkat, mert az eredmény az életünk minőségét javítja." A privacy jogának társadalmi rendeltetése visszájára fordul Schneier gondolatmenetében.[56] A fogyasztói magatartás logikáját és eredményét szemléletesen ragadja meg.

Az előzőekben áttekintettük a magánszféra születése és a technológia kapcsolatát. Bemutattuk, hogy a védelmi deficit végigkíséri a technológia fejlődését, ezért a védelem folyamatos kiigazításra, erősítésre szorul. De egyáltalán: mit tekintünk védelemnek? A Rendelet egyes jogintézményeinek részletes vizsgálata előtt szükséges megfogalmazni azt, hogy mit értünk védelmen, milyen módon épül fel az adatvédelem szabályozása. Mindennek fényében tudjuk majd elemezni az egyes jogintézmények szerepét a védelmi szint megőrzésében, illetve erősítésében.

A magánszférához fűződő jog

Az egyedüllétre vágyó ember a technológia korábbi fejlettsége mellett másként élte meg a közösségi létet és az egyedüllétet. Onnantól kezdve, hogy kívül szeretett volna maradni a fényképezőgépek látókörén, igénye támadt a másoktól, vagy még inkább: a technológia által lehetővé tett tolakodástól zavartalan életre. (A technológia fejlődésének számos olyan vívmánya van, amely szintén befolyásolta az emberek magánszféráját. Más példák is felhozhatók lennének, mint a távíró vagy a telefon, azonban a privacygondolkodásban a gyors exponálású fényképezőgépek hatása vezetett a leglátványosabb jogi eredményekhez.) Azóta az embernek van alapja azzal számolni, hogy nincs egyedül. Önmagában a technikai eszköz, az első időszakban a fényképezőgép jelenléte, is kiváltja az igényt a védelemre. Ez az igény tehát a kiindulópontunk, ezt a vágyat már jogi értelemben is meg lehet

[55] Aleecia M. McDonald: When Self-help Helps: User Adoption of Privacy Technologies. In Marc Rothenberg – Julia Horwitz – Jeramie Scott (szerk.): *Privacy in the Modern Age – the Search for Solutions*. New York, The New Press, 2015. 127–137.

[56] Bruce Schneier: Fear and Convenience. In Rothenberg–Horwitz–Scott (2015): i. m. 201.

ragadni. Jogi elismertetése a 19. század végén megfogalmazódott, míg az adatvédelmi normák csak évtizedekkel később, több, egymást követő szabályozási generációban születtek meg. A 20. századi adatvédelmi szabályok különböző korszakolására születtek kísérletek. Jóri András részletesen és szemléletesen mutatja be ezeket a generációkat, és a szabályozás három nagy korszakát különbözteti meg.[57]

Az egyedülléthez való jog az élet minőségével mutat összefüggést. Itt nem az élet fizikai védelméről vagy az egészséget veszélyeztető körülményekről, hanem arról van szó, hogy az életet megőrizzük *élvezhetőnek*.[58] Olyan feltételeket kell tehát teremteni, ahol a jog alanya igényt támaszthat a zavarás esetén annak elhárítására, és ezt egy külső szereplő beavatkozása révén el is érheti. Mindjárt meg is jelenik a köz- és a magánérdek közötti mérlegelés gondolata, hiszen vannak személyek és vannak élethelyzetek, amikor a magánérdekkel szemben a köz érdeke élvez elsőbbséget. (Az Emberi Jogok Európai Bírósága által vizsgált Von Hannover I és II ügyek e két érdek mérlegeléséről szólnak, továbbá szintén e mérlegelést végzik el a később idézendő egyéb, Strasbourgban született ítéletek is.) Ettől még a jogosultság tartalma azonos, legfeljebb az adott körülmények között korlátozhatóvá válik. A jog lényege a kivételektől függetlenül világosan megfogalmazható.

Az egyedülléthez való jog nem csupán „emberi" vágy. Alan Westin a privacy igényének elemzése kapcsán arra mutat rá, hogy az állatvilágban is megfigyelhető az igény olyan időszakokra, amikor az egyed egyedül vagy kis csoportjában kíván maradni. A biztonságot nyújtó területüket is megvédik: nemcsak az emlősök, de a madarak és a halak esetében is megfigyelhető ez.[59]

A magam részéről a magánszférát az embert körülvevő, tőle el nem választható közegnek tekintem, amelybe belépni, betekinteni csak a jog által meghatározott módon, terjedelemben és célból megengedett. A magánszférának különböző dimenziói[60] léteznek. (A dimenziók megkülönböztetése végigkíséri a privacy jogával foglalkozó irodalmat. Bloustein például pszichológiai, társadalmi és politikai dimenziókat különböztet meg, és el is ismeri,

[57] Jóri András: *Adatvédelmi kézikönyv*. Budapest, Osiris Kiadó, 2005. 21–66. A Rendelet e generációs felosztás szerint a legkésőbbi, harmadik korszakba tartozik.

[58] Brandeis–Warren (1890): i. m. 193.

[59] Westin (1984): i. m. 56–57.

[60] Edward J. Bloustein: Privacy as an Aspect of Human Dignity – An Answer to Dean Prosser. In Shoeman (1984): i. m. 157.

hogy ezek aztán messze túlmutatnak a jogi elemzésen.) A magánszféra fizikai dimenziója arra a térre, területre utal, amely az egészséges és teljes élethez szükséges. Ez az igény nem csupán az ember számára nélkülözhetetlen, ugyanezt az állatvilágban is megfigyelhetjük. A pszichológiai dimenzió a másik ember általi megfigyeltséggel mutat összefüggést. A másik figyelme hatással van az egyén magatartására.

A magánszféra pszichológiai dimenzióját illetően talán leegyszerűsítő az elemzésünk. Kétségtelen, hogy a privacy kapcsán számos emberi érzés szerepet játszhat. Bruce Schneier a megfigyelések és a túlzott adatgyűjtések kapcsán mutat rá arra, hogy a félelem is fontos lehet a magánszférába benyomuló megfigyelések elfogadásában. „A technológiáról tanácskozunk, miközben nem veszünk tudomást a pszichológiáról. És amíg a privacy minden bizonnyal technológiai probléma is, sokkal inkább emberi probléma."[61]

Akkor élhető meg a magánszféra teljessége, ha nem kell a másik ember figyelmével számolni. Végül a virtuális dimenzió minden olyan digitálisan rögzített adatra utal, amelynek kezelése az egyént vagy a róla kialakított képet valamilyen formában befolyásolhatja. Az egyes ügyek kapcsán valamely dimenzió hangsúlyosabb lehet, elemzésemben azonban a magánszféra dimenzióit egységesen, egységes egészként kezelem.[62]

[61] Schneier (2015): i. m. 200.

[62] Vö. Szabó Endre Győző: Adatvédelem és technológia. In Klein Tamás – Tóth András (szerk.): *Technológia jog – Robotjog – Cyberjog.* Budapest, Wolters Kluwer Hungary Kft., 2018. 26.

A Rendeletben védett jog tartalma és terjedelme az emberi jogok európai egyezményének fényében

Az előzőekben bemutattam a magánszférával kapcsolatos jogfejlődés egyes elemeit, a privacy jogának születését és az adatok védelmének jelentőségét mindezek kontextusában. A következőkben azt vizsgálom, hogy a magánszférát az Európai Unió milyen módon határozza meg jogi értelemben, milyen adatvédelmi keretet határoz meg a magánszféra védelme érdekében. Ennek kapcsán elemezni fogom az emberi jogok európai egyezményében (a későbbiekben: EEJE, illetve Egyezmény) rögzített, a magánélet védelmével összefüggő esetjogot is.

A védelem szintjének kérdései az Európai Unió Alapjogi chartájában

A Rendelet a charta által védett jogok kontextusában szabályozza a személyes adatok védelmének kérdéseit. A szabályozás átfogó, a védelem valamennyi kérdését rendezni kívánja. Az átfogó jellegen túl nemzetközi dimenziója is markáns, hiszen szabályait az Európai Unió, valamint az Európai Gazdasági Térség valamennyi tagállamában közvetlenül kell alkalmazni, az irányultsági szabályok révén pedig még az unió területén kívül is alkalmazandóvá válik a Rendelet szabályrendszere, gyakorlatilag a világ bármely pontján.

Bár a Rendelet kifejezetten nem említi a szabályozás alapjogi hátterét, az az elsődleges jog alapján meghatározható. Az Európai Unió működéséről szóló szerződés (EUMSZ) 16. cikke szerint mindenkinek joga van a rá vonatkozó személyes adatok védelméhez. Az adatok védelmére és az ilyen adatok szabad áramlására vonatkozó jogalkotási felhatalmazást szintén ez a cikk adja meg. Az EUMSZ rögzíti, hogy e szabályok tiszteletben tartását független hatóságok ellenőrzik.[63]

Az Európai Unió Alapjogi chartája 7. cikkében előírja, hogy mindenkinek joga van ahhoz, hogy magán- és családi életét, otthonát és kapcsolattartását

[63] Az EUMSZ nem határozza meg a felügyeleti hatóságokra vonatkozó további szabályokat, azt csak évekkel később a Rendelet részletezi.

tiszteletben tartsák. A 8. cikk szerint mindenkinek joga van a rá vonatkozó személyes adatok védelméhez. A charta szerint a személyes adatokat csak tisztességesen és jóhiszeműen, meghatározott célokra, az érintett személy hozzájárulása alapján vagy valamilyen más, a törvényben rögzített jogos okból lehet kezelni. Mindenkinek joga van ahhoz, hogy a róla gyűjtött adatokat megismerje, és joga van azokat kijavíttatni.[64] A személyes adatok védelméhez fűződő jog tiszteletben tartását független hatóságnak kell ellenőriznie.[65]

A charta a saját rendelkezéseinek értelmezésére is iránymutatást ad.[66] Az 52. cikk (3) bekezdése szerint amennyiben a charta olyan jogokat tartalmaz, „amelyek megfelelnek az emberi jogok és alapvető szabadságok védelméről szóló európai egyezményben biztosított jogoknak", akkor a jogok tartalmát és terjedelmét „azonosnak kell tekinteni azokéval, amelyek az említett egyezményben szerepelnek". Annak megelőzése érdekében, hogy egyfajta védelmi plafont jelentsen ez a szabály, a charta azt is rögzíti, hogy ez a rendelkezés nem akadályozza meg azt, hogy az unió joga kiterjedtebb védelmet nyújtson. Az emberi jogok európai egyezménye, valamint az Emberi Jogok Európai Bíróságának (EJEB, Bíróság) joggyakorlata tehát minimum védelmi szintként értelmezhető.

A védelem jogszabályokban rögzített összetevőit és szintjét elemzem. Abban a kérdésben, hogy a védelem mely szintje lenne ideális, gyakorlatilag minden tagállamban más és más válaszra jutnánk, ahogyan ezt a Rendeletet megelőző időszak bizonyította. Nem beszélhetünk tehát arról, hogy az Európai Unióban megvalósul a védelem „ideális szintje", hanem egy olyan védelemről beszélhetünk, amely a jog tartalmát illetően kompromisszumot élvez. Az eszményi, vagy ha úgy tetszik, láthatatlan mérce jogi elemzésem során figyelmen kívül marad, mindazonáltal a védelem szintje tekintetében nincs védelmi „plafon". A védelem szintjének romlása egyértelműen kimutatható és kifogásolandó. Ez a munka is ennek a törekvésnek a jegyében született.

[64] A charta 8. cikkének (2) bekezdése szerint.

[65] A charta 8. cikkének (3) bekezdése szerint. Nem csupán az Európai Unió joga, hanem az Európa Tanács úgynevezett 108-as egyezményének kiegészítő jegyzőkönyve (CETS 181, 2001) is elvárja a tagállamoktól a független adatvédelmi felügyeleti szerv létrehozását.

[66] A charta I–VI. címei alatt rögzíti a jogokat, szabadságokat és elveket, a VII. cím pedig „A Charta értelmezésére és alkalmazására vonatkozó általános rendelkezések" címet viseli.

Felmerülhet a kérdés, hogy a Rendelet értelmezésével foglalkozó munka miért szentel teret, az Európai Unió jogalkotási aktusa szerint védendő jog kapcsán, az Európa Tanács jogvédelmi rendszerének. A válasz röviden akként adható meg, hogy a Rendelet maga nem határozza meg e jog tartalmát. A preambulumbekezdések sem nyújtanak iránymutatást arra nézve, hogy a jogalkotó szerint a személyes adatok védelme milyen alapokon áll és milyen terjedelemben nyújtandó. A Rendelet nem szól a védelem alapjául szolgáló rendszertani háttérről. Az EUMSZ 16. cikke önmagában kevés eligazítást nyújt a védelem terjedelmét illetően, ezért szükségesnek tartom az Egyezmény, valamint az annak alapján kialakult esetjog elemzését úgy is, mint minimum védelmi szintet.

Az alábbi kitekintésben az Emberi Jogok Európai Bíróságának azon ítéleteit vizsgálom meg, amelyek a charta által hivatkozott „tartalom és terjedelem" körében az Európai Unió joggyakorlatában is alkalmazandó védelmi szintre nézve is meghatározók.

A magánélet fogalmának meghatározása az Emberi Jogok Európai Bíróságának esetjogában

Mielőtt az esetjog feldolgozásába kezdenék, szükséges a magánélet és a személyes adatok védelmére irányuló egyezmények rendszerét bemutatni.

Egyezmények által biztosított jogi keret

A Rómában 1950. november 4-én aláírt egyezmény az emberi jogok és alapvető szabadságok védelméről 8. cikkében rögzíti a magán- és családi élet tiszteletben tartásához való jogot.

1948-ban írták alá az Emberi jogok egyetemes nyilatkozatát, amely a 12. cikkében rögzíti a magánélet tiszteletben tartásához való jogot: „Senkinek magánéletébe, családi ügyeibe, lakóhelye megválasztásába vagy levelezésébe nem szabad önkényesen beavatkozni, sem pedig becsületében vagy jó hírnevében megsérteni. Minden személynek joga van az ilyen beavatkozásokkal vagy sértésekkel szemben a törvény védelméhez." A nyilatkozat hatást gyakorolt a jogi gondolkodásra és nemzetközi törekvésekre, így az egyezményre is.

A cikk szerint mindenkinek joga van arra, hogy magán- és családi életét, lakását és levelezését tiszteletben tartsák. Bár a 8. cikk kifejezetten nem említi a személyes adatok kezelését és védelmét – ami egy 1950-ben született dokumentum kapcsán nem is tekinthető meglepőnek –, az Egyezmény érvényesülését elősegíteni hivatott Emberi Jogok Európai Bírósága (EJEB) fogad olyan kérelmeket, amelyek a 8. cikk körében a személyes adatok jogellenes kezelését kifogásolják. A Bíróság gyakorlatában olyan esetjog alakult ki az elmúlt évtizedekben, amelyekből kiolvashatók a charta által hivatkozott standardok, nevezetesen a jog tartalmára és terjedelmére vonatkozó elvárások. Menyhárd Attila is hangsúlyozza az esetjog feldolgozásának szükségességét, szerinte a magánélethez való jog tartalmi meghatározása és a jogvédelem határainak megvonása kapcsán az EJEB értelmező tevékenysége lehet az egyetlen támpont ahhoz, hogy a magánélethez való jog egységes értelmezést kapjon Európában.[67]

Az Európa Tanácsnak az egyének védelméről a személyes adatok gépi feldolgozása során, Strasbourgban, 1981. január 28. napján kelt egyezménye[68] (az úgynevezett 108-as egyezmény) a személyes adatok védelmének részletes szabályait határozta meg. A 108-as egyezmény egyértelműen az emberi jogok európai egyezményének 8. cikkéhez kapcsolódik, azonban a Bíróság az egyezmény körébe tartozó ügyekben nem hoz döntéseket. Ez a hatásköri korlát fájó hiányosság az európai adatvédelemben, hiszen ilyen módon a 108-as egyezmény strasbourgi bírói gyakorlata nem alakulhat ki. Az ítéletek tehát nem egy átfogó adatvédelmi keret elemzéséből fakadnak, hanem a magánélet körében értékelendő adatkezelések jogszerűségének (*Az emberi jogok európai egyezményével* való összhangjának) elbírálása révén, esetről esetre alakítanak ki standardokat. Látni fogjuk, hogy az ítélkezési gyakorlat koherens és következetes, mindazonáltal az ügyek tematikája sporadikus képet mutat.

[67] Menyhárd Attila: A magánélethez való jog a szólás- és médiaszabadság tükrében. In Csehi Zoltán – Koltay András – Navratyil Zoltán (szerk.): *A személyiség és a média a polgári és a büntetőjogban – Az új Polgári Törvénykönyvre és az új Büntető Törvénykönyvre tekintettel*. Budapest, Wolters Kluwer Complex Kiadó, 2014. 201.

[68] Máig az egyetlen kötelező erejű, adatvédelmi tárgyú nemzetközi egyezmény.

A Bíróság több ítéletében is elemezte a magánélet fogalmát, és arra jutott, hogy nem lehetséges annak pontos és kimerítő definícióját megadni. Erre a következtetésre jut Menyhárd is, aki polgári jogi megközelítést alkalmazva úgy fogalmaz, „aligha van a jognak homályosabb fogalma, mint a magánélethez való jog".[69] Még ennél is borúlátóbb Ronald J. Krotoszynski, aki szerint a privacy egy változatos fogalom, ami úgy tűnik, hogy mindent jelent – és semmit – egy időben,[70] vagy egy amerikai szövetségi bíró, aki a privacyt egy szénakazalhoz hasonlította a hurrikánban.[71]

A magánélet meghatározása során széles alkalmazási kört állapít meg a Bíróság, amibe beletartozik a személyes fejlődésnek (a személyiség szabad kibontakoztatásának) aspektusa, a személyes autonómia védelme. Menyhárd a magánélet védelme alá vonható jogokat összekötő kapocsként az emberi méltóság védelmét és az egyéni szabadságot említi.[72] A magánélet körébe tartozik az egyén társadalmi identitása, nemi önazonossága, neve, szexuális irányultsága és szexuális élete. A családhoz való kötődése, vagy az egészségével kapcsolatos információk, ahogyan az etnikai hovatartozása is, a magánélet fontos elemeként tartandó számon.[73]

A Bíróság elismeri, hogy mindenkinek joga van az életét mások nem kívánt figyelme nélkül élni. A magánélet fogalmának túlzott korlátozása lenne, ha a magánéletet csak egy „belső kör" tekintetében értelmeznénk, ennek megfelelően a magánélet joga magában foglalja a „társadalmi magánélet" területét is.[74] Ez pedig a másokkal való érintkezés szabadságát,

[69] Menyhárd (2014): i. m. 177.

[70] Ronald J. Krotoszynski Jr.: *Privacy Revisited – A Global Perspective on the Right to Be Left Alone*. Oxford University Press, 2016. 2–3.

[71] Edward J. Bloustein idézi a bírót, aki az Ettore v. Philco Television Broadcasting Co. ügyben fogalmazott így a privacy jogát illetően: „The state of the law is still that of a haystack in a hurricane but certain words and phrases stick out." Bloustein (1984): i. m. 156.

[72] Menyhárd (2014): i. m. 179.

[73] S. and Marper v. Egyesült Királyság, no. 30562/04 és 30566/04, 2008. december 4-i ítélet, 66. §.

[74] „Social private life" a strasbourgi bíráskodásban. A López Ribalda és mások v. Spanyolország ügyben született, 2019. október 17-i ítélet, 88. és 103. §. A koncepció lényege, hogy a magánélet nem csupán egy „belső körre" szűkül, hanem annak van egy társas dimenziója is, ahol az egyén másokkal alakíthat ki kapcsolatokat. Ez a szféra pedig a szakmai életben is megjelenik, amint arra a Fernández Martínez v. Spanyolország-ügy is rámutat.No. 56030/07, § 110, ECHR 2014.

a kapcsolatok szabad alakításának szabadságát is magában foglalja.[75] A kiskorúak személyiségfejlődése és társadalmi beilleszkedése különösen fontos szempont a magánélettel összefüggő kérdések vizsgálata során.[76]

A magánélet nem csupán a szó „privát" körében értelmezhető, hanem munkahelyi közegben is. A munkahelyről indított és ott fogadott magánjellegű telefonhívások így a magánélet körébe tartoznak. Az érintettnek a munkahelyi környezetben is van jogos elvárása a magánéletének tiszteletben tartásával kapcsolatban.[77] Sőt, a Bíróság elismeri, hogy a munkahelyen kifejezetten széles lehetőség nyílik a személyes kapcsolatok alakítására, amely a magánélet védelmének e körre való kiterjesztését indokolja.[78]

A magánélet körébe tartozik a személy fizikai és pszichológiai integritása is.[79] Az egyénről a társadalomban kialakított kép, a reputáció is a 8. cikk által védett jogok körébe tartozik a Bíróság szerint.[80]

Az ítélkezési gyakorlat a védelmet olyan esetekre is kiterjesztette, amikor a magánéletbe való beavatkozás nem bizonyítható, de az állam, különösen a titkos információszerzés, a kommunikáció lehallgatása révén bizonytalanságba sodorja állampolgárait, és ez kihat a magánélettel kapcsolatos várakozásokra. Ilyen esetekben a Bíróság elfogadja, hogy gyakorlatilag bárki a magánéletének megsértése révén „áldozattá" válik, ezért ezen a területen részletes érveléssel dolgozta ki a szerződő államokkal szembeni elvárásokat.[81] A Bíróság a védelem mérlegelése során tekintettel van a változó technológiai környezetre is. Nem hunyhat szemet például a büntetőeljárások során alkalmazott eszközöknek az érintettek magánéletére gyakorolt hatásának vizsgálatakor afölött, hogy egyre fejlettebb eszközök állnak a nyomozó hatóságok rendelkezésére, és ezért a magánéletbe való beavatkozás minősége is változik. A köz- és a magánérdek gondos mérlegelésére van szükség az új technológiai lehetőségek (például a genetikai azonosítás) alkalmazása során.[82]

[75] Bărbulescu v. Románia, no. 61496/08, 2017. szeptember 5-i ítélet, 70. §.
[76] S. and Marper v. Egyesült Királyság, no. 30562/04 és 30566/04, 2008. december 4-i ítélet, 124. §.
[77] Halford v. Egyesült Királyság, no. 20605/92, 1997. június 25-i ítélet, 44–45. §.
[78] Bărbulescu v. Románia, no. 61496/08, 2017. szeptember 5-i ítélet, 71. §.
[79] Söderman v. Svédország, no. 5786/08, 2013. november 12-i ítélet, 80. §.
[80] Petrenco v. Moldova, no. 20928/05, 2010. március 30-án kelt ítélet, 44. §.
[81] Klass and others v. Németország, no. 5029/71, 1978. szeptember 6-i ítélet, 34–36. §, valamint Szabó és Vissy v. Magyarország, no. 37138/14. 2016. január 12-i ítélet, 33–34. §.
[82] S. and Marper v. Egyesült Királyság, no. 30562/04 és 30566/04, 2008. december 4-i ítélet, 112. §.

A személyes adatok kezelése a 8. cikkben rögzített jogba való beavatkozásnak minősül.

A magánélet fogalma az egyén azonosíthatóságához kapcsolódó körülményeket, így a személy nevét, a róla készült képmásokat, a fizikai és a morális sérthetetlenségét is felöleli. A másokkal való érintkezés szabadságának birtokában, ami teret ad a személyiség fejlődésére, egy olyan zónaként, szféraként is értékelhető, amelynek van egy nyilvános, nem csupán privát kontextusa. Ennek alapján hivatkozhatnak a magánélet jogára olyan személyek is, akik egyébként közszereplőnek tekintendők.[83] Az „átlagos személyek" esetében az érintkezés szabad zónája, illetve ennek igénye tágabb körben ismerendő el, és az a tény, hogy az érintett ellen büntetőeljárás van folyamatban, nem szűkíti e jog terjedelmét.[84]

Az egyén arcképmása a személy egyik legfontosabb ismertetőjegye, szorosan kötődik a személyiségéhez, hiszen feltárja egyéni jellemzőit, amelyek másoktól megkülönböztetik. A személyiség fejlődésének és védelmének lényeges eleméről van szó a felvételek védelme során.[85] A Bíróság a fényképekhez hasonlóan a hangminták és az ujjnyomatok esetében is megállapította a magánélet érintettségét.[86]

Az azonosítható természetes személyről szóló adatok tárolása egy közhatalmi szervnél a 8. cikk hatálya alá tartozik, az adatok puszta tárolása már a magánéletbe való beavatkozásnak minősül.[87] Vonatkozik ez a titkosan kezelt adatállományok tárolására és az azokból való adattovábbításra is. Sőt, még az egyébként nyilvános adatok kezelése is a 8. cikk alá esik abban az esetben, ha a hatóságok szisztematikus módon gyűjtik az adatokat az érintettről. Annál inkább igaz ez, minél távolabbi múltját érinti az adatok alanyának.[88] A hatóságok által tárolt adatok érintett általi cáfolhatóságának elutasítása szintén a magánélethez való jogba történő beavatkozásnak minősül.[89]

[83] Von Hannover v. Németország (No. 2), no. 40660/08 és 60641/08, 2012. február 7-i ítélet, 95. §.
[84] Sciacca v. Olaszország, no. 50774/99. 2005. január 11-i ítélet, 29. §.
[85] Von Hannover v. Németország (No. 2), 96–97. §.
[86] S. and Marper v. Egyesült Királyság, 84. §.
[87] S. and Marper v. Egyesült Királyság, 67. §.
[88] Rotaru v. Románia, no. 28341/95, 2000. május 4-i ítélet, 43. §.
[89] Rotaru v. Románia, 46. §.

A Bíróság nem tesz különbséget érzékeny és kevésbé érzékeny adatok között, mindegyik esetében megállapítható a beavatkozás ténye. Mindazonáltal az adatok természete és mennyisége szerepet játszik abban, hogy az államnak milyen védelmi kötelezettségei származnak az adatok kezeléséből. Az emberi sejtekből és a DNS-mintából nyerhető adatok értelemszerűen fokozott állami védelmet igényelnek.[90] A genetikai adatokból a vérségi kapcsolatokra is következtetéseket lehet levonni, ami tovább erősíti a védelem igényét.[91]

Az egészségügyi adatok védelme különösen fontos a Bíróság értékelése szerint annak érdekében, hogy a magánéletbe való jogellenes beavatkozás elkerülhető legyen. Amennyiben az ilyen adatok jogellenesen elérhetővé válnak mások számára, az érintettek bizalma meginog az intézmények iránt, és adott esetben nem merik feltárni azokat az orvosok előtt. Fertőző betegségek esetén ez különösen nagy kockázatot jelent.

A HIV-fertőzésre utaló információ esetében a védelem igénye még inkább fokozott, ennek kiszivárgása drámaian érintheti az egyén családi és társadalmi életét.[92] Az ilyen adat nyilvánosságra hozásának mérlegelése során figyelmet kell szentelni annak, hogy az adat hozzájárul-e egy demokratikus társadalomban zajló vitához, vagy inkább csak egy személlyel kapcsolatos cifra találgatások forrásaként értékelhető. Utóbbi esetben értelemszerűen a köz érdeke nem túlnyomó a magánérdekkel szemben.[93] A Bíróság szintén vizsgálja, hogy a jogkorlátozásra a jogban való rögzítettség mellett kerül-e sor. Az érdekmérlegelést ilyen esetekben a jogalkotó társadalmi szinten már elvégezte.[94]

Az Emberi Jogok Európai Bíróságának joggyakorlata szerint az adatkezelés vizsgálata során a „joggal összhangban" kifejezés utal egyrészt arra az elvárásra, hogy valamilyen jogalapra *(some basis in domestic law)* támaszkodjon az adatkezelő, másrészt pedig a jog minőségére nézve is követelményt támaszt *(quality of the law),* tehát a jog előírása elérhető annak címzettje számára, és a hatásai előreláthatóak.

[90] S. and Marper v. Egyesült Királyság, 73. §.
[91] S. and Marper v. Egyesült Királyság, 75. §.
[92] Z. v. Finnország, no. 9/1996/626/811, 1997. január 25-i ítélet, 95–96. §.
[93] Biriuk v. Litvánia, no. 23373/03, 2009. február 25-i ítélet, 38. §.
[94] Amann v. Svájc, no. 27798/95, 2000. február 16-i ítélet, 50. §.

Az állam pozitív és negatív kötelezettségeiről

A Bíróság az előtte zajló eljárásokban elsősorban azt vizsgálja, hogy a szerződő államok magatartása révén sérülnek-e az Egyezményben rögzített jogok. A Bíróság elismeri, hogy ez elsősorban arra kötelezi az államokat, hogy tartózkodjanak az Egyezmény aktív megsértésétől. A Bíróság azt is vizsgálja azonban, hogy amennyiben a magánélettel összefüggő vita magánfelek között alakul ki, akkor az állam eleget tesz-e azon kötelezettségének, hogy megfelelő intézkedéseket tegyen a magánélet védelme érdekében.[95] A joggyakorlat szerint ugyanis a 8. cikk alapján nem csupán passzív, hanem aktív kötelezettségei is vannak az államnak a magán- és családi élet tiszteletben tartása terén.[96]

Ez a kötelezettség értelmezhető például az érintett fényképével való visszaélés megakadályozására is.[97] Súlyos esetekben arra is kiterjed, hogy büntetőjogi védelmet nyújtsanak, és ilyen módon rettentsék el a jogsértésre készülőt az elkövetéstől. Bár ezen a téren a tagállamoknak van mozgásterük az Egyezménynek való megfelelés módjának megválasztásában, a Bíróság tekintettel van a szerződő államokban kialakult egyező irányú tendenciákra, és ezt ítélkezési gyakorlatában is figyelembe veszi.[98] Az érzékenyebb személyi körbe tartozók esetében, például a gyerekeknél a magánélethez fűződő jog megsértésének megakadályozása még markánsabban megjelenő kötelezettség.[99]

A jogsértésnek el kell érnie egy olyan szintet, amelynek megvalósulása esetén a szerződő államon számon lehet már kérni a beavatkozás elmulasztását. Ezzel a Bíróság elismeri, hogy a jogsértésnek kellően komolynak kell lennie. (Nyilvánvalóan átlépte ezt a küszöböt az a jogsértés, amikor egy gyermek arcképének felhasználásával hoztak létre egy profilt a társkereső oldalon, kitéve ezzel a pedofiloktól származó kapcsolatfelvételnek a fiatalt.)[100] Ennek hiányában a Bíróság nem állapítja meg az Egyezmény sérelmét. Ez a teszt egy küszöbnek tekinthető, amely küszöb alá eső sérelmek esetében a jogsértést nem állapítja meg a Bíróság.

[95] Söderman v. Svédország, 78. §.

[96] *Handbook on European Data Protection Law*. Luxemburg, European Union Agency for Fundamental Rights, Council of Europe, 2014. 15.

[97] Von Hannover v. Németország (No. 2), 98. §.

[98] K. U. v. Finnország, no. 2872/02, 2009. március 2-i ítélet, 43–44. §.

[99] Söderman v. Svédország, 81. §

[100] K. U. v. Finnország, 45. §.

Az államok pozitív és negatív kötelezettségeinek érvényesítésekor a strasbourgi bíráskodás tehát a vertikális jogvédelem mellett a horizontális jogvédelmet is számonkéri a tagállamokon. Ez a bírósági hozzáállás a védelem szempontjából jelentős szemléleti kérdés több okból is. Egyrészt, amint láttuk, a 108-as egyezményre nem terjed ki a Bíróság hatásköre, másrészt pedig ilyen módon olyan esetjog is alakul, amely a Rendelet alkalmazása során, a charta idézett rendelkezései révén, szintén zsinórmértékül szolgál.

Ez a strasbourgi bíráskodásról szóló rövid áttekintés bemutatta, hogy az Egyezmény alapján kibontakozó esetjog nem alkalmas a személyes adatok védelméhez fűződő jog rendszerszerű megalapozására. Mindazonáltal értékes mércét és tájékozódási pontokat nyújt a védelem és annak szintje vizsgálatához, úgy is mint az Európai Unióban érvényesítendő minimum védelmi szint.

A személyes adatok védelméhez fűződő jog – a horizontális jogvédelem kérdései

Elemzésemben nem csupán itt érintem a horizontális jogvédelem kérdéseit. Az EJEB esetjogának feldolgozása során említek olyan jogeseteket, amelyekben nem csupán az állam negatív, hanem pozitív kötelezettségeit is vizsgálta a Bíróság, nevezetesen azt, hogy a 8. cikkben garantált jog magánfelek közötti érvényesülése érdekében az állam nem mulasztotta-e el valamely pozitív kötelezettségét.

Az emberi jogok magánjogi jogviszonyokban való érvényesülését a jogirodalom már részletesen elemezte. A kérdésfelvetés lényege abban áll, hogy az emberi jogok érvényesülését csak a nemzetközi egyezményekben részes államoknak, a polgáraikhoz fűződő vertikális jogviszonyokban kell-e érvényesíteniük, vagy ezek a magánjogi szereplők között is érvényre kell hogy jussanak.

Menyhárd arról értekezik, hogy ezt a kérdést a német jogtudomány több évtizedes vitában részletesen megválaszolta, és a német szerzők között konszenzus alakult ki abban, hogy az alkotmányos követelmények a generális klauzulák révén érvényesülnek a magánjogi jogviszonyokban *(mittelbare Drittwirkung).*[101] Az említett vitán túl Menyhárd úgy látja, hogy a „magánjog valós modellje" hordozza a felvetett kérdésekre a választ. Ezt a modellt

[101] Menyhárd (2014): i. m. 202.

alkalmazva az emberi jogok „valójában azt a közös európai értékrendet adják meg, amelyek a társadalmi együttélés alapvető követelményeit rögzítik”.[102] Akár közvetetten, akár közvetlenül tehát, teszem hozzá a magam részéről, az alapjogi katalógusban rögzített jogok hatást és érvényesülést követelnek mind a horizontális, mind a vertikális jogviszonyokban.

A Polgári törvénykönyvről szóló 2013. évi V. törvény szerint a törvény rendelkezéseit Magyarország alkotmányos rendjével összhangban kell értelmezni.[103] Az Alkotmánybíróság vonatkozó ítélkezési gyakorlata fogalmazta meg a horizontális hatály követelményét, először a 8/2014. (III. 20.) AB határozatban.[104] Gárdos-Orosz Fruzsina és Bedő Renáta vonatkozó elemzésükben kiemelik, hogy az Alkotmánybíróság szerint a bíróságoknak alkalmazniuk kell az Alaptörvény rendelkezéseit a jogviták elbírálása során.[105] Munkajogi jogviszonyt vizsgálva is jutott hasonló következtetésre az Alkotmánybíróság, mégpedig hogy a szerződéses szabadság tiszteletben tartása mellett a bíróságnak a generálklauzulákat az Alaptörvényre tekintettel kell értelmeznie.[106]

A személyes adatok védelméhez fűződő jog sajátos fejlődési utat járt be a többi alapvető joggal összehasonlítva. A *The Right to Privacy* című írás 1890-ben (Warren és Brandeis) a technológia meg nem engedett használatát kifogásolva kifejezetten magánjogi viszonyban követelte az új jog, az egyedüllét jogának védelmét. Kétségtelen, hogy az USA jogrendszerében természetesebb a kötődés az alkotmányjogi követelmények és a magánjogi jogérvényesítés között, a horizontális jogvédelem kérdései a kontinentális jogfejlődésben élesebb kérdéseket vetnek fel. Ami az adatvédelmet illeti, születése időpontjától fogva természetes, hogy abszolút szerkezetű jog, az egyén mindenkivel szemben megfogalmazott igénye, hogy egyedül hagyják. *Bárki* lehet az, aki ezt a választott magányt megzavarhatja.

Az adatvédelem jogi generációinak egyik elhatárolási szempontja a hatály kérdése. Akkor, amikor csupán az állam, és néhány kivételesen

[102] Menyhárd (2014): i. m. 203–204.

[103] Polgári törvénykönyv (Ptk.) 1:2. § (1) bekezdés.

[104] Az Alkotmánybíróság több más határozatában is hivatkozott a horizontális jogvédelem elvére, így a devizahiteles ügyben született 34/2014. (XI. 14.) AB határozatban, vagy a 3/2015. (II. 2.) AB határozatban.

[105] Gárdos-Orosz Fruzsina – Bedő Renáta: Az alapvető jogok érvényesítése a magánjogi jogviták során – az újabb alkotmánybírósági gyakorlat (2014–2018). *Alkotmánybírósági Szemle,* 1. (2018), 1. 3–15.

[106] Gárdos-Orosz – Bedő (2018): i. m. 9.

nagy üzleti szereplő volt képes olyan számítógépeket fenntartani, amellyel kapcsolatban a védelmet meg akarták fogalmazni, a személyi hatály csupán rájuk, ezekre a nagy szereplőkre terjedt ki. Természetesen adódott a technológiához szorosan kapcsolódó jogfejlődés során a személyi hatály kiterjesztése. Ma *bárki* lehet adatkezelő, ennek technológiai feltételei magától értetődőek. Ezért a jogalkotó természetesen döntött amellett, hogy a közjogi és magánjogi jogviszonyokra egyaránt alkalmazandónak tartja a Rendelet szabályait, jelentős különbségtétel nélkül.

A közjogi és a magánjogi adatkezelők között nincsenek lényeges különbségek az általános kötelezettségek terén, de tetten érhető a különbségtétel például az adatvédelmi tisztviselő kinevezése, a bírságolás, a közhatalmi szervek privilegizált helyzete, vagy éppen a jogalapok korlátozott alkalmazásának lehetősége esetében.

A Rendeletet megelőző tagállami szabályozások és maga a 95/46/EK adatvédelmi irányelv is ezt a szabályozási modellt követte.

Azt látjuk tehát, hogy a horizontális jogvédelem igénye az adatvédelmen túl más alapjogok esetében is elvárásként fogalmazódik meg. A személyes adatok terén ilyen vita nem bontakozott ki, a jogfejlődés minden szükséges magyarázat nélkül terjesztette ki az érintettet megillető és az adatkezelőt, adatfeldolgozót terhelő jogokat a magánjogi viszonyokra. Az adatvédelmi felügyeleti hatóság feladatainak ellátásában leírt szemléleti változás a horizontális védelem igényét természetesnek tekinti, az állami felügyelet intézményét pedig aktívabb szerepre biztatja. E szerepmódosítás egy célt szolgál: a személyes adatok védelméhez, illetve a magánszférához fűződő jog hatékonyabb érvényesülését. Azt, hogy az adatkezelők és az adatvédelmi hatóságok – kiegészülve egy sokkal erősebb szerepben dolgozó adatvédelmi tisztviselővel – a mindennapi viszonyokban érvényesítsék a jogszabályban előírtakat. Mindezt úgy, hogy az erőforrások optimális felhasználása mellett a lehető legmagasabb szinten érvényesüljön a személyes adatok védelme.

A védendő jog mibenléte a Rendelet alapján

Az előzőekben azt elemeztem, hogy az EEJE, valamint az annak alapján kialakított esetjog alapján mi az a minimumvédelem, amelyet a magánélet/magánszféra körében a személyes adatokra tekintettel elemzésem alapjának tekintek. Amint bemutattam, a strasbourgi esetjog a charta tekintetében minimum védelmi szintként határozható meg. Ez a minimum védelmi szint pedig értelemszerűen az egész uniós jog, így a Rendelet alkalmazása tekintetében is irányadó. Az alábbiakban a Rendelet által biztosított szabályozás rendszerét tekintem át.

A Rendelet értelmezési kerete

Az értelmezési keret a Rendelet esetében is az alapjogi dokumentumokban rögzített jog, nevezetesen a személyes adatok védelméhez fűződő jog.[107] Megjegyzendő, hogy a Rendelet normaszövege nem hivatkozik a magánélethez fűződő jogra mint a személyes adatvédelemnél szélesebb körű védelemre. Figyelemre méltó változás ez, hiszen a Rendelet által hatályon kívül helyezett 95/46/EK számú irányelv még kifejezetten hivatkozott rá.

> A 95/46EK számú irányelv 1. cikkének (1) bekezdése az irányelv céljaként a következőket határozta meg: „A tagállamok ezen irányelvnek megfelelően védik a természetes személyek alapvető jogait és szabadságait, különösen a magánélet tiszteletben tartásához való jogukat a személyes adatok feldolgozása tekintetében."

A magánélet jogára való hivatkozás csupán a (4) preambulumbekezdésben merül fel, és ott is azoknak a jogoknak a csokrában, amelyeket a jogalkotó szem előtt tart a Rendelet alkalmazásakor.[108]

[107] Az Európai Unió *Alapjogi chartája,* 8. cikk és az Európai Unió működéséről szóló szerződés, 16. cikk.

[108] Annál is inkább hiányolható a hivatkozás, mert az Európai Bizottság 2010. novemberi közleménye még a *Magánélet védelme az összekapcsolódó világban 21. századi európai adatvédelmi keret* címet viselte. Ez a közlemény pedig már a Rendelet előkészítésének keretében született.

Jogalkotói cél, hogy a személyes adatok kezelését az emberiség szolgálatába kell állítani.[109] A közjó megjelenítése és érvényesítése helyeselhető, hiszen morális értéktartalmat társít a formális jogi érvelések mellé. A technológiának az ember szolgálatába állítása és az emberközpontú szabályozásának az igénye már korán felmerült Isaac Asimov robottörvényeiben.

> A jól ismert törvények a következő beszélgetés során hangzanak el: „– Ide figyelj, Mike – recsegett Powell izgatott hangja Donovan fülhallgatójában –, kezdjük az elején, a robotika három törvényével. A három törvénnyel, amely teljesen átitatja a pozitronagyat. – Kesztyűbe bújtatott ujjain számolt a sötétben. – Íme! Egy: a robotnak nem szabad kárt okoznia emberi lényben, vagy tétlenül tűrnie, hogy emberi lény bármilyen kárt szenvedjen. – Helyes. – Kettő – folytatta Powell –: a robot engedelmeskedni tartozik az emberi lények utasításainak, kivéve, ha ezek az utasítások az első törvény előírásaiba ütköznének. – Helyes. – És három: a robot tartozik saját védelméről gondoskodni, amennyiben ez nem ütközik az első és második törvény előírásaiba." [110]

Az erős morális jogalkotói alapvetésen túl azt is megállapíthatjuk, hogy a Rendelet a személyes adatok védelmére vonatkozó szabályokat nem helyezi más jog kontextusába, csupán abban nyújt eligazítást, hogy mely más jogokra tekintettel kell értelmezni az általa nyújtott védelmet. Az adatok védelméhez való jog egyébként sem abszolút, az arányosság elvével összhangban, a „társadalomban betöltött szerepének függvényében kell figyelembe venni", más jogokkal egyensúlyra törekedve.

> E jogok a magán- és családi élet védelme, az otthon és a kapcsolattartás tiszteletben tartásához, a gondolat-, a lelkiismeret- és vallásszabadsághoz való jog, a véleménynyilvánítás és a tájékozódás szabadságához való jog, a vállalkozás szabadságához, hatékony jogorvoslathoz, a tisztességes eljáráshoz, a kulturális, vallási és nyelvi sokféleséghez való jog (Rendelet [4] preambulumbekezdés). A társadalomban betöltött szerepre való utalás az Európa Tanács modernizált Egyezményének preambulumában is megjelenik.

[109] A Rendelet (4) preambulumbekezdésének első mondata.

[110] Isaac Asimov: Körbe-körbe. In *Robottörténetek*. Budapest, Móra Ferenc Ifjúsági Könyvkiadó, 1982.

Az EU helyzetéből adódik, hogy itt szuverén tagállamokon átívelő szabályozásról van szó, amely még komplexebbé teszi a szabályozott életviszonyokat. Ezek a körülmények rávilágítanak arra, hogy minél bonyolultabb a szabályozás, illetve minél összetettebb kontextusban kell majd annak érvényesülni, annál fontosabb az elvi alapvetés, amelyre a szabályozás épül.

A Rendelet magát a védendő alapjogot nem jelöli meg sehol, nem hivatkozik még a magánszféra védelmére sem, csak a személyes adatok védelmét határozza meg a norma céljaként. Ahol mégis tetten érhetjük a jogalkotói szándék szerint védendő jog körvonalait, azok a kockázatok leírásában keresendők, egész pontosan a (75) preambulumbekezdésben. Itt írja körül a jogalkotó, hogy milyen kockázatoktól kell megóvni a védelemben részesülőket. Úgy is fogalmazhatunk, hogy nem pozitív, hanem negatív módon határozza meg a Rendelet mögött álló és védendő értékeket.

A kockázatok sokrétűek, az adatok nem jogszerű kezelése fizikai, vagyoni vagy nem vagyoni károkhoz vezethet, különösen, ha „az adatkezelésből hátrányos megkülönböztetés, személyazonosság-lopás vagy személyazonossággal való visszaélés, pénzügyi veszteség, a jó hírnév sérelme, a szakmai titoktartási kötelezettség által védett személyes adatok bizalmas jellegének sérülése, az álnevesítés engedély nélkül történő feloldása, vagy bármilyen egyéb jelentős gazdasági vagy szociális hátrány fakadhat”.[111] Hasonlóan kockázatot jelent, ha az érintettek nem gyakorolhatják jogaikat, vagy nem rendelkezhetnek saját személyes adataik felett.[112]

Különös kockázatot jelent olyan személyes adatok kezelése, amelyek a különleges adat kategóriába tartoznak, így faji vagy etnikai származásra, politikai véleményre, vallási vagy világnézeti meggyőződésre, illetve szakszervezeti tagságra utalnak. Hasonlóan fokozott védelmet igényelnek a genetikai, egészségügyi adatok vagy a szexuális életre, büntetőjogi felelősség megállapítására, illetve bűncselekményekre, vagy ezekhez kapcsolódó biztonsági intézkedésekre vonatkozó adatok.

Az adatvédelmi jog nevesíti a személyes jellemzők értékelésére irányuló adatkezeléseket mint fokozott kockázattal járó műveleteket (így különösen munkahelyi teljesítménnyel kapcsolatos jellemzők, gazdasági helyzet,

[111] Idézet a Rendelet (75) preambulumbekezdéséből.

[112] Itt gyakorlatilag az információs önrendelkezési jog sérül, amely a német szövetségi alkotmánybíróság 1983-as Volkszählung ítélete (Urteil des Bundesverfassungsgerichts vom 15. Dezember 1983, Az.: 1 BvR 209/83, 1 BvR 269/83, 1 BvR 362/83, 1 BvR 420/83, 1 BvR 440/83, 1 BvR 484/83) óta az európai adatvédelem egyik központi gondolatává vált.

egészségi állapot, személyes preferenciák vagy érdeklődési körök, megbízhatóság vagy viselkedés, tartózkodási hely vagy mozgás elemzésére vagy előrejelzésére szolgáló adatkezeléseket), amelyek során személyes profil létrehozása vagy felhasználása történik. Érzékenyebb társadalmi csoportba tartozó személyek (gyermekek, idősek, fogyatékkal élők) személyes adatainak kezelése, vagy ha egyébként is nagy mennyiségű vagy nagyszámú érintettre terjed ki a műveletsor, a kockázatok társadalmi és jogi értelemben is nagyobbak.

Mindezekre és a folyamatosan fejlődő technológia, továbbá az új üzleti modellek által támasztott kihívásokra tekintettel egy újra meg újra megújuló-erősödő jogszabályi védelemre van szükség. Ezen túl a következetes hatósági és bírósági joggyakorlat is alapvető igénye a jogvédelemnek, amelynek jogfejlesztő hatása is van. A Google- vagy a Schrems-ügy nyomán például jelentős változások történtek az európai uniós adatvédelemben. A Google-ügy az internet világában a felejtés lehetőségét teremtette meg, míg a Schrems-ügy a harmadik országba irányuló adattovábbítások terén a védelmi szint megfelelőségét garantáló jogi keret újjáépítéséhez vezetett.

Az alapjogi háttér mellett számontartandó a Rendelet szerepe a közös piacon a személyes adatok szabad áramlásának megteremtésében. E két funkció nincs egymással hierarchikus viszonyban, mindvégig a jogalkotó egyenrangú célkitűzései maradnak. Gyakorlati megfontolás áll a háttérben, nevezetesen az, hogy a közös piac működéséhez elengedhetetlen személyes adatok szükség szerinti elérhetőségét és áramlását csak a piaci szereplők magatartásának szabályozása révén lehet elérni.

Az adatok védelme és a közös piac kérdései legutóbb például az *Európa digitális jövőjének megtervezése* című bizottsági közleményben jelent meg. E szerint „[a]z adatok ma már a termelés kulcsfontosságú tényezőjét képezik, és az általuk létrehozott értéket újra meg kell osztani a társadalom egészével, amely rendelkezésre bocsátotta azokat. Ezért kell kiépítenünk a valódi egységes európai adatpiacot – az európai szabályokon és értékeken alapuló európai adatpiacot."[113]

[113] A Bizottság közleménye az Európai Parlamentnek, a Tanácsnak, az Európai Gazdasági és Szociális Bizottságnak és a Régiók Bizottságának: *Európa digitális jövőjének megtervezése*. Brüsszel, COM(2020)67 végleges, 9. (2020. február 19.)

Ez a megfontolás vezet el a harmonizált szabályok igényéhez, és azonnal hozzá kell tennünk az egységes alkalmazást, amely folyamatos erőfeszítést igényel a jogalkalmazók részéről. A szabad áramlás előfeltétele a magas és mindenütt azonos módon garantált védelmi szint. A védelmi szint különbözőségeire hivatkozással nem is engedélyezett az adatok áramlásának akadályozása az Európai Gazdasági Térségen belül.

A Rendelet (13) preambulumbekezdése szerint „[a] belső piac megfelelő működése érdekében a személyes adatok Unión belüli szabad áramlását a természetes személyeknek a személyes adatok kezelése tekintetében történő védelmével összefüggő okokból nem szabad korlátozni vagy megtiltani". Ez a szempont már a 2016/680/EU bűnügyi irányelvben is megjelenik, amely az Európai Unió pillérrendszerének felszámolásával is magyarázható jogfejlődés.

A Rendelet elemzésének kiindulópontjai

Az Európai Unió általános adatvédelmi Rendelete 2018. május 25-étől alkalmazandó. A Rendelet azzal a jogalkotói szándékkal született meg, hogy széles körben és magas szinten nyújtson védelmet a természetes személyeknek személyes adataik kezelése kapcsán. Az Európai Unió Bíróságának esetjoga megerősíti ezt a jogalkotói szándékot, az adatvédelmi szabályok egyik fontos értelmezési szempontjaként tekint a magas védelmi szintre.[114] A magas védelmi szint mellett a közös gazdasági térségben biztosítani szeretnék a személyes adatok szabad áramlását, ami a gazdasági és egyéb kapcsolatok érdekében nélkülözhetetlen.

A Rendelet (10) preambulumbekezdésének első mondata szerint „[a] természetes személyek következetes és magas szintű védelmének biztosítása és a személyes adatok Unión belüli áramlása előtti akadályok elhárítása érdekében a természetes személyeknek az ilyen adatok kezelésével összefüggésben fennálló jogait és szabadságait minden tagállamban azonos szintű védelemben kell részesíteni".

E két célkitűzés, a védelem és a szabad áramlás azonos súlyú célok, ezeknek egymásra tekintettel, egy időben kell érvényesülniük.

[114] Lásd például a 2014. december 11-i Ryneš-ítélet 27. pontját, valamint az ott hivatkozott ítélkezési gyakorlatot, C-212/13, EU:C:2014:2428.

A Rendelet a tárgyáról szóló cikkében rögzíti, hogy a Rendelet a természetes személyek védelmére vonatkozik a személyes adatok kezelése tekintetében. E védelem mellett a személyes adatok szabad áramlására vonatkozó szabályokat állapít meg. A jog védelme nem csupán a tagállamokban, hanem az Európai Unióban is a legmagasabb szinten rögzített. Magyarországon az Alaptörvény VI. cikke garantálja mindenki számára a jogot személyes adatai védelméhez. Az Európai Unió Alapjogi chartája 8. cikkének (1) bekezdése írja elő, hogy „mindenkinek joga van a rá vonatkozó személyes adatok védelméhez". Tartalmában azonos rendelkezést tartalmaz az Európai Unió működéséről szóló szerződés 16. cikkének (1) bekezdése. Az Európai Unió működéséről szóló szerződéshez Lisszabonban fűzött jegyzőkönyv szerint az Európai Unió Alapjogi chartája, amely jogilag kötelező erővel bír, megerősíti az alapvető jogokat úgy, ahogyan azokat az emberi jogok és alapvető szabadságok védelméről szóló európai egyezmény biztosítja, és ahogyan azok a tagállamok közös alkotmányos hagyományaiból erednek. A védendő jog tartalmát illetően tehát több forrás és tájékozódási pont is rendelkezésre áll, egyrészt az Emberi Jogok Európai Bíróságának ítéletei, másrészt pedig a tagállami jogok és az ezekhez kapcsolódó joggyakorlat.

A Rendelet általános jellegéből fakadóan a bűnügyi irányelv által nem szabályozott területeken gyakorlatilag minden jogviszonyban alkalmazandó. Értelemszerű kivételt jelentenek ez alól azok a szabályozási tárgykörök, amelyek az Európai Unió jogának hatályán kívül esnek, mint például a nemzetbiztonsági kérdések, de ez sem jelentős szűkítés, hiszen többek között az eredetileg üzleti célból tárolt, majd később nemzetbiztonsági célból felhasználható adatok kezelésére is a Rendeletet kell alkalmazni az adatkezelés első szakaszában. Abban az esetben, ha például egy bank tranzakciókhoz kötődő adatokat kezel, ez a Rendelet hatálya alatt történik, függetlenül attól, hogy esetlegesen később a nemzetbiztonsági szolgálatok a banktól adatokat igényelnek. Az ilyen adatok kezelése csupán a nemzetbiztonsági szervek körében kerül majd kívül a Rendelet tárgyi és személyi hatályán, csak abban az esetben tehát, ha mind a két feltétel teljesül: az általános adatvédelmi Rendeletnek sem a tárgyi, sem a személyi hatálya nem terjed ki a vizsgált adatkezelésre. A hatály tehát általános, és ennek megfelelően számos jogterületen érvényesül a Rendelet alkalmazásának kötelezettsége.

A Rendelet 2. cikkének (2) bekezdése szerint a Rendelet nem alkalmazandó a személyes adatok kezelésére:
– ha az uniós jog hatályán kívül eső tevékenységek során végzik,

– vagy a tagállamok az Európai Unió működéséről szóló szerződés V. címe 2. fejezete szerint a határok ellenőrzésével, a menekültüggyel és a bevándorlással kapcsolatos politikák körében kezelnek adatokat.

Továbbá nem terjed ki a Rendelet hatálya azokra az adatkezelésekre, amelyeket természetes személyek kizárólag személyes vagy otthoni tevékenységük keretében végeznek.

Végül értelemszerűen kívül esik a Rendelet alkalmazási körén a bűnügyi irányelv hatálya alá tartozó tevékenységekhez kötődő adatkezelés, amennyiben mind a személyi, mind a tárgyi hatály szerint kívül esik az általános adatvédelmi rendelet alkalmazásán.

A Rendelet áttekintő elemzése

A Rendelet szabályai három nagy blokkban mutathatók be.

a) A jogok és kötelezettségek rendszere

Az első a jogok és kötelezettségek rendszere. Idetartozik az alapelvekre, a jogalapokra, az érintetti jogokra, az adatkezelő és az adatfeldolgozó felelősségére, az adatbiztonságra (ideértve az adatbiztonsági incidens kezelését is), az adatvédelmi hatásvizsgálatra, az adatvédelmi tisztviselőre, az önszabályozás eszközeire (magatartási kódex és tanúsítás) vonatkozó szabályozás.[115]

b) Az alkalmazási kör

A második a hatály kérdése, illetve az alkalmazási kör: mikor, kire, milyen feltételekkel kell alkalmazni az első blokkban említett szabályokat. E blokkba tartozik a Rendelet tárgyára, hatályára vonatkozó szabályozás, a fogalom-meghatározások, a személyes adatok különleges kategóriáit meghatározó rendelkezések, és idesorolandó a harmadik országba irányuló adattovábbítás szabályrendszere is, amelynek funkciója a védelem kiterjesztése unión kívüli területekre.[116]

[115] A Rendelet 5–42. cikkei.

[116] A Rendelet 1–4. cikkei, a 9–10 cikkek bizonyos rendelkezései és a 44–50. cikkek.

c) A kikényszerítés eszközei és intézményei

A harmadik blokkba pedig a kikényszerítés eszközei és intézményei tartoznak – azt, hogy melyek azok az ügyek, amelyekben ezek használhatóak, az első két blokk alapján állapítható meg. A szabályok közül e területre esik a felügyeleti hatóságok illetékességére, feladataira és hatáskörére, a hatóságok együttműködésére, valamint az Európai Adatvédelmi Testületre vonatkozó szabályozás.[117]

A három blokk egyike sem áll meg önmagában, csak együttesen értelmezhetők: a védelem rendszere hiányos lenne bármelyik szabályozási egység nélkül.

A három blokkba tartozó valamennyi résztéma elemzésére terjedelmi korlátokból kifolyólag nincsen mód, ezért szükségszerű, hogy előre meghatározott szempontok szerint kell dönteni a részletezendő témákról. Hatósági jogalkalmazóként a gyakorlati szempontokat is figyelembe vettem az egyes kérdések kiválasztása során. E szempont megjelenése természetesen adódik a szerző és a téma kapcsolatából.

Álláspontom szerint az érintettek jogainak érvényesítésére a legnagyobb hatást az adatkezelői magatartás gyakorolja. Ebben jut kulcsszerep – helyes jogalkalmazás esetén – az adatvédelmi tisztviselőnek. A védelem rendszere pedig elképzelhetetlen az adatvédelmi felügyeleti szerv létrehozása nélkül. E két komponens alkotja a védelem központi intézményi elemeit. A következőkben kifejtendő védelmi lépcső elméletét a tisztviselőre és az adatvédelmi hatóságra alkalmazva értekezem arról, hogy a Rendelet tárgyalt intézményei miként illeszkednek a védelmet alakító komponensek közé.

Az adatvédelmi tisztviselő és a hatóság elemzését megelőzően azt vizsgálom, hogy melyek a védelem komponensei, milyen szabályozási elemekből áll a védelem rendszere. Általános módon tekintem át a Rendelet szabályozási elemeit, és a védelem szintjére gyakorolt hatását tárgyalom absztrakt módon. A munka következő fázisa a későbbi fejezetekben következik, amikor az egyes jogintézményekre vonatkozó szabályozást és a védelem szintjének alakulását állítom az elemzés középpontjába.

[117] A Rendelet 51–84. cikkei.

A védelem komponensei és a védelem szintjének kérdései a Rendelet szabályozásában – a védelmi lépcső elmélete

A következőkben azt vizsgálom, hogy a védelem építőkövei és garanciái milyen módon jelennek meg az Európai Unió általános adatvédelmi Rendeletében. Ebben a fejezetben egy vázlatos, de teljességre törekvő áttekintést nyújtok azokról a szabályozási elemekről, amelyek a védelem szintjére hatást gyakorolnak.

A kontextus

A jogi gondolkodásban mindig jelentős eredményként tartjuk számon azokat a teszteket, amelyek révén egy-egy jogkérdés tágabb kontextusban, világos, generálisan alkalmazható kérdések révén megválaszolható. Ezek fontos fogódzót jelentenek a könnyebb és a nehezebb ügyek megítélésében is. Ilyen eredmény például az alapjogi korlátozások kapcsán a szükségességi-arányossági teszt.

Annak érdekében, hogy a védelem szintjét helyesen fel tudjuk mérni, a szükséges intézkedéseket, kiigazításokat meg tudjuk tenni, a védelmi lépcső elméletét kínálom. Ennek az elméletnek a kidolgozására és néhány kiválasztott intézményre való alkalmazására teszek kísérletet az alábbiakban.

A védelmi lépcső gondolata szintén az esetről esetre való elemzést segíti elő azáltal, hogy kontextusba helyezi a védelmi komponenseket, amelyek kombinációjától végső soron a védelem szintje függ. A védelmi lépcső első megközelítésben egyszerű. Egymást követő, és a védelem minőségének szintjét mutató lineáris fokozatok láncolataként határozhatjuk meg.

Az adatvédelmi jog generációi

A nemzetközi kitekintés alapján azonosíthatók a védelem kialakulásának fokozatai, majd annak erősödése. Így itt említhetjük meg a privacy

jogának születését, az adatvédelmi szabályok generációinak alakulását,[118] az Európa Tanács, majd az EU jogalkotását, majd mindezeket követően eljutunk a Rendelethez, amelyet a jogi védelem legmagasabb ismert fokának tekinthetünk. Ez a lépcsőzetesség helyesen mutatja be a szabályozás alakulását, azonban túlzottan leegyszerűsítené a szabályozás elemeiből összeálló védelmet. A védelmi lépcső ugyanis nem nagy blokkokból áll, hanem sok apró elem kombinációjából adódik össze, és ezek a kombinációk fogják megmutatni, hogy összességében milyen minőségű az a védelem, amely az adott államban az érintettek számára elérhető. Célom ezeknek az építőelemeknek az azonosítása. Az említett fokozatosság a szabályozás történetében leginkább a szabályozás generációival írható le, de ezt nem tekinthetjük a védelmi lépcső kidolgozott fokozatainak. Azért sem, mert nem feltétlenül fejezik ki helyesen a védelem minőségének alakulását, inkább egyfajta korszakolásnak tekinthető.

A védelem komponensei és fokozatai

A védelem eróziója vagy fejlődése nem feltétlenül nagy és látványos intézkedésekből adódik össze. Éppen ez a jogi elemzés célja, hogy azonosítsa azokat a pontokat, ahol a védelem indikátorai megtalálhatók. A védelem egyes komponensei inkább statikusak, mint például az adatvédelmi szabályozás a következő módosításig, vagy a hatóságok léte. Ezek megalkotása szükségszerűen része a védelem struktúrájának, a védelem minőségéről önmagukban is sokat mondanak. A védelem nem a statikus elemek ideális struktúrát követő összeillesztéséből, hanem sokkal inkább a privacyt érintő kockázatokhoz dinamikusan alkalmazkodni képes rendszer létrehozatalából áll. A védelmi lépcső ebben a megközelítésben már sokkal komplexebb elemzést kínál: ahhoz ad támpontot, hogy a nagyobb kép egyes részleteiben is megtalálja azokat az összetevőket, amelyek látszólag talán nem jelentősek, módosításuk, vagy éppen elavulásuk mégis kihat a védelem szintjére.

[118] A szabályozás generációinak összehasonlítására tesz kísérletet Szőke Gergely László, aki írásában áttekinti a tárgyban korábban született magyar írásokat. Majtényi László, Jóri András és Hegedűs Bulcsú is gyakorlatilag három szabályozási generációt különböztet meg, de némiképp eltérő szempontok szerint. Szőke Gergely László: Az adatvédelem szabályozásának történeti áttekintése. *Infokommunikáció és Jog,* 56. (2013), 3. 107–112.

A lépcső gondolata annak lehetőségét kínálja, hogy azon felfelé és lefelé is vezet az út. Az új jogalkotás nem feltétlenül jelent minden esetben előrelépést a lépcsőn, hanem könnyen elképzelhető, hogy egyes elemeiben visszalépésként értékelendő.

A védelmi lépcső fokozatainak azonosítása

A védelmi lépcsőn álláspontom szerint nem szükséges sok fokozat azonosítása. A lépcső elméletében természetesen egy felfelé a végtelenbe mutató, lineáris lépcsőt képzelhetünk el, amely a védelem javulásának és alkalmazkodásának kifogyhatatlan lehetőségét jeleníti meg a jövőben. Egzakt módon sem a lefelé, sem a felfelé vezető fokok nem határozhatók meg nagy számban. Nincs is erre szükség, az elemzés szempontjából három szint meghatározása azonban elengedhetetlen. Az egyik az a fokozat, amelyen a védelem szintje jelenleg megragadható. A másik az, amelyikről a jelenlegi szintre felfelé, vagy éppen lefelé lépett a védelem. A harmadik szint pedig a kívánatos, előrelépésnek tekinthető védelem szintje. Nem lényeges, hogy a szintek között mekkora a különbség, akár egy kisebb minőségi javulás is új szintként azonosítható. Az szükséges, hogy a kettő között a különbséget egyértelműen meg tudjuk határozni. Emellett az is másodlagos, hogy a védelmi szintek közötti előrelépés egy szerves fejlődés eredménye, vagy például egy teljesen új intézmény meghonosításában áll.

Miben látható a minőségi különbség két fokozat között? E tekintetben számos tényező jöhet szóba. A minőségi javulás indikátora lehet, ha az érintett jogai bővülnek, vagy a jogok változatlan katalógusa mellett is javul a jogérvényesítés lehetősége. Amikor az érintett számára elérhető információk köre bővül, vagy a szabályozás e tekintetben világosabb követelményeket határoz meg, az szintén minőségi javulást eredményez.

Az előrelépés jellemzője, hogy az adatkezelőket az adatkezelés kapcsán terhelő kötelezettségek az alkalmazott technológia és az üzleti modellek fényében fejlődnek. Szándékosan kerülöm a kötelezettségek bővülésének említését, mert a védelmi lépcső nem mennyiségi, hanem minőségi fokmérő. Az adatkezelések általános bejelentési kötelezettsége például a védelemre nem hatott pozitívan, ehelyett azonban az adatvédelmi incidensek bejelentési kötelezettsége érdemben javít a védelem állapotán. A Rendelet tárgyalásai során az incidensek bejelentésének kötelezettsége az egyik olyan újításként jelent meg, amely a korábbi védelmi szinthez képest előrelépést

ígért.[119] Az adatkezelő szervezetén belül a dedikált adatvédelmi szakértelem megjelenése, a kontrollmechanizmusok erősödése szintén minőségi változás.

Az adatvédelmi hatóságok mozgástere, feladat- és hatásköre szintén minőségi jellemzője a védelem szintjének. Nem feltétlenül valamiféle maximalista szemléletet tartok itt helyesnek, tehát minél szélesebb a felügyeleti hatóságok hatásköre, annál magasabb a védelem szintje. Itt sem mennyiségi kérdéseket taglalok, ugyanakkor helyesnek tartom, ha széles körű a hatóságok mozgástere. Mark H. Moore figyelmeztetésével, amely szerint a közszférában a növekedés nem mindig kívánatos, egyetértek.[120] Álláspontom szerint ugyanakkor a jogfejlődés jelenlegi szakaszában egyszerre van jelen a mennyiségi és a minőségi változások szükségessége. Ennek megfelelően a hatóságok feladatainak, hatásköreinek bővülését önmagában is minőségi változásnak tekintem, a kivételeket külön említeni és indokolni szükséges.

A minőségi előrelépés megmutatkozhat a jog hatékonyságában is. Amint másutt kitérek rá, az adatvédelmi jog hatékonyságának jogi fokmérője, hogy a magánszféra védelme erősödik, fejlődik. Amennyiben ez megvalósul, úgy a védelmi lépcsőn előrelépés történik.

A minőségi fejlődés fontos fokmérője, hogy az adott változás képes-e hozzájárulni az adatvédelmi kultúra kialakulásához, illetve fejlődéséhez. Az adatvédelmi kultúrát olyan „táptalajnak" tekintem, amelyben az adatvédelmi előírások természetesen vezetnek magasabb magánszféra-védelemhez egy alacsonyabb adatvédelmi kultúrát megjelenítő közeggel összehasonlítva.

Az előrelépés lehetőségei a védelmi lépcsőn

A védelmi lépcső elméletének sajátossága, hogy abban a „fordított gravitáció" érvényesül. Egy demokratikus társadalomban, jogállami kereteket feltételezve természetesen adódik az a jogalkotói törekvés, hogy a védelem szintjét folyamatosan javítsák, karbantartsák. Ezzel természetesen együtt jár az arról való gondolkodás, hogy a védelmet milyen módon lehet a következő időszakban javítani, erősíteni. Ennek megfelelően a jogalkotói cél folyama-

[119] Péterfalvi Attila – Szabó Endre Győző: Hol tart az Európai Unió adatvédelmi reformja? *Acta Humana,* 4. (2014), 2. 7–12.

[120] Mark H. Moore: *Creating Public Value: Strategic Management in Government*. Cambridge, Massachusetts, Harvard University Press, 1995. 72.

tosan előre, illetve felfelé irányul, és ezért mindig a védelmi lépcsőn való feljebb jutás a kézenfekvő irány. Bár a lépcsőn vezet út lefelé, mindig a felfelé vezető út az, ami nem igényel különösebb indoklást. Következésképpen ez a helyes és természetes irány, a jogalkotásban érvényesülő nehézkedés a védelmi lépcsőn felfelé mutat.

Az egyes komponenseket nem szemlélhetjük azok statikus voltában. Egy adatkezelési vagy adatvédelmi szabály adott időpillanatban tűnhet korszerűnek, néhány év múlva azonban már elavul, vagy adott esetben kifejezetten károssá is válhat. A szabályozás rendszeres felülvizsgálata a száguldó technológiai fejlődés mellett elkerülhetetlen. A Rendelet 97. cikke azt írja elő az Európai Bizottság számára, hogy első ízben 2020. május 25-ig, majd azt követően négyévente készítsen jelentést a Rendelet értékeléséről és felülvizsgálatáról.[121] Egy-egy alkotóelem kiesése a rendszerből nem minden esetben jár visszalépéssel. Sőt a hatékony védelmet korlátozó elemek jogból való kivezetése kifejezetten kedvezően hat a védelem alakulására.

A védelmi lépcső elméletét alkalmazva nem feltétlenül lehet egy egész közösség, például egy ország vagy egy kontinens védelmi szintjét precízen leírni. Adatkezelő szervezetenként változik a védelem szintje. Adott esetben egy jól menedzselt szervezetet is érinthet súlyos adatvédelmi incidens, jelentős következményekkel. Még nagyobb az esélye annak, hogy egy rosszul vezetetett szervezeten belül nagyobb számban fordulnak elő jogsértések. Ennek aspektusaira nézve az adatvédelmi bírság kiszabása során figyelembe vett szempontok nyújtanak támpontot.

A védelem szintjét jogi megközelítés szerint vizsgálom. Tisztában vagyok azzal, hogy a védelem szintjének értelmezésében léteznek eltérő megközelítések, amelyek a GDPR-tól eltérő modellt kínálnak ugyanannak a célnak az elérésére. Azt a jogalkotó is elismeri, hogy a személyes adatok védelméhez fűződő jog nem abszolút, azt az arányosság elvével összhangban, más alapvető jogokra is tekintettel kell figyelembe venni.

[121] Az Európai Bizottság 2020. június 24-én hozta nyilvánosságra az értékelés eredményeként a következő két dokumentumot. A Bizottság közleménye az Európai Parlamentnek és a Tanácsnak: *A polgárok szerepe erősítésének és az EU digitális átállással kapcsolatos megközelítésének pillérét képező adatvédelem – az általános adatvédelmi rendelet alkalmazásának két éve.* (COM[2020]264 végleges). *Eur-lex.europa.eu;* és *Commission Staff Working Document, Accompanying the Document. 'Communication from the Commission to the European Parliament and the Council, Data Protection as a Pillar of Citizen's Empowerment and the EU's Approach to the Digital Transition – Two Years of Application of the General Data Protection Regulation'.* (SWD2020)115 végleges. *Eur-lex.europa.eu*.

A GDPR (4) preambulumbekezdése szerint „ez a rendelet minden alapvető jogot tiszteletben tart, és szem előtt tartja a Chartában elismert és a Szerződésekben rögzített szabadságokat és elveket".

Kétségtelen az is, hogy a GDPR az érintetti jogokat nem azok gazdasági kontextusában vizsgálja. Ennek következménye az, hogy elemzésemben erre én sem térek ki. A gazdasági szempontok egyébként a Rendelet fényében nem csupán az EU-ban, hanem az EU piacán tevékenykedni kívánók körében is élénk érdeklődésre tartanak számot. He Li, Lu Yu és Wu He szerint például az amerikai és kínai vállalatok a megfelelés költségeinek következményeként versenyhátrányba kerülnek.[122]

A GDPR kapcsán a jogalkotót az a vád is érte, hogy az új rendelet a gazdaságot torzító eredményre vezet, hiszen a túlontúl erősen definiált érintetti jogok, nevezetesen a hozzájárulás visszavonása és a törléshez való jog az adatok kezelőinél anyagilag is mérhető bizonytalanságot hoznak magukkal. Az értékes piaci adatok kezelői egy bizonytalan közegben kénytelenek működni, holott kidolgozható és alkalmazható lenne olyan innovatív informatikai-gazdasági modell, amely kevesebb adatkezeléssel járna, egyszersmind stabilabb piaci körülményeket teremtene.[123]

Potts és szerzőtársai a blockchain-technológia nyújtotta lehetőségekben látják az egyik megoldást, amelynek alkalmazásával az érintett erősebb védelemre, az adatkezelő pedig nagyobb gazdasági biztonságra, valamint kiszámíthatóbb jogi környezetre számíthatna. Ezzel kiküszöbölhető lenne például a GDPR egyik hátrányos mellékhatása, mégpedig az, hogy az adatokat kezelő szervezetek biztosítást lennének kénytelenek kötni az érintetti joggyakorlás hátrányos gazdasági hatásainak ellensúlyozására. Azért is figyelemre méltó a felvetés, mert a blockchain-technológiát a GDPR-ral való összeegyeztethetetlensége miatt övezi bizonytalanság. Potts és szerzőtársai ezzel ellentétben kifejezetten erre építenének fel egy privacybarát konstrukciót.

[122] Vö. He Li – Lu Yu – Wu He: The Impact of GDPR on Global Technology Development. *Journal of Global Information Technology Management,* 22. (2019), 1. 1–6.
[123] Allen Darcy et al.: Some Economic Consequences of the GDPR. *Economics Bulletin,* 39. (2019), 2. 785–797.

Tekintettel arra, hogy az elemzés kereteit meghaladná e téma mélyebb tárgyalása, annak említésén túl, hogy az EU által kínált védelmi rendszertől eltérő modellek is elképzelhetők, például a kevesebb szabályozás révén, részletesebben nem térek ki.

Az állam kiemelt felelőssége

Az adatkezelések és az adatkezelők említésekor az államok felelősségét külön is említeni kell. A jogalkotáson túl az állami adatkezelések menedzselése nyújtja annak a mintának a bemutatását, amely szélesebb körben is példaként szolgálhat, és amelynek révén a normakövetés is erősebb legitimációval kérhető számon az állam által létrehozott adatvédelmi hatóságok munkája, vagy éppen a bíróságok eljárása során.

A normakövetés és az adatvédelmi kultúra összefüggései

A védelmet leíró jellemzők sokasága alapján egy széttöredezett kép alakulhat ki. Ez teljesen természetes, hiszen sok tényező egyidejű értékeléséről van szó, amelyek jelentős része nem statikus, hanem több szempontból is dinamikus környezetben vizsgálandó, ráadásul adatkezelő szervezetről adatkezelő szervezetre változó képet mutathat. Sőt, mindezek összességeként, ha egy új távlatot is megnyitunk a védelem értékelésben, azt látjuk, hogy mindezek eredőjeként egy olyan jelenségről szólhatunk, amit adatvédelmi kultúrának szoktunk nevezni.

Visegrády Antal meghatározását elemzésem tárgyára alkalmazva úgy fogalmazhatunk, hogy az adatkezelők és adatfeldolgozók jogkövetésre való hajlandóságát a „jogszabályok célkitűzéseivel összhangban alakító jogi kultúra" elősegíti, ellenkező esetben pedig csökkenti.[124] A cél az olyan adatvédelmi kultúra megteremtése, amely egymást erősítő lépésekből jelentős erővé válik, végeredményben a hatékony jogérvényesítést és a magánszféra védelmének magas szintjét támogatja.

[124] Visegrády Antal: A jogi kultúra és a joghatékonyság keretei. *JURA,* 23. (2017), 2. 239.

A védelem szintjének folyamatos javítására, vagy legalábbis szinten tartására tett erőfeszítések nem választhatók el a jog hatékonyságának kérdéseitől. A 29. cikk szerinti munkacsoport alapján az adatkezelőknek kell biztosítaniuk azt, hogy a „gyakorlati intézkedések valóban hatékonyak" legyenek.[125] A védelem szintje akkor javul, ha a jog érvényesül, és a jogalkotó által kitűzött célok végső soron megvalósulnak.

A jog hatékonyságának kérdéseit az elmúlt évszázadokban a jogirodalom részletesen tárgyalta. Visegrády áttekintése a külföldi és hazai szakirodalom legfontosabb szerzőiről és elméleteiről[126] a jog és a társadalom, valamint a jogi kultúra kontextusában vizsgálja a jog hatékonyságának körülményeit. A Visegrády által idézett Reinhold Zippelius szerint a „jogi normák oly mértékben hatékonyak, amennyiben a velük kitűzött jogpolitikai célt elérik. Ez a hatékonyság két komponenstől függ: egyrészt attól, hogy a normákat figyelembe veszik-e, másrészt attól, hogy az előírt magatartás a normacél elérésének megfelelő eszköze-e". Az adatvédelmi jog hatékonysága témánk szempontjából azt jelenti, hogy a Rendelet betartása, illetve betartatása révén a magánszférához fűződő jog érvényesül.

A védelem kapcsán szóba kell hozni az ellenőrizhetőség hiányában megnyilvánuló deficitet. Walter Barfuss szerint a nem hatékony normák egyik típusa az olyan jogszabály, amelynek végrehajtása komolyan nem ellenőrizhető.[127] A technológia sajátosságaiból adódóan láthatatlan adatokon végzett nehezen bizonyítható műveletek világában az adatvédelmi szabályok hatékonysága bizony e mérce szerint is megközelíthető, és ezt is észben kell tartani akkor, amikor a védelem szintjének erősítését, vagy más szóval az adatvédelmi jog hatékonyságának javulását szeretnénk elérni, ennek jövőbeni útját meghatározni.

Szilágyi Péter idézi Kulcsár Kálmánt, aki szerint a jog hatékonysága azonos a társadalmi viszonyokban való megvalósulásával.[128] Szilágyi rámu-

[125] A 29. cikk szerinti munkacsoport 3/2010 számú véleménye az elszámoltathatóság elvéről, elfogadás időpontja: 2010. július 13. 10. Forrás: az Európai Bizottság (a 29. cikk szerinti Munkacsoport titkárságának) honlapja.

[126] Visegrády (2017): i. m. 238–254.

[127] Visegrády (2017): i. m. 245.

[128] Szilágyi Péter: Jogbölcseleti mozaikok a jog hatékonysága kapcsán. In Nochta Tibor – Monori Gábor (szerk.): *Ius Est Ars. Ünnepi tanulmányok Visegrády Antal professzor 65. születésnapja tiszteletére.* Pécs, PTE ÁJK, 2015. 472.

tat arra is, hogy a joglépcsőelmélettel ismertté vált Hans Kelsen a jog hatékonyságával kapcsolatos korábbi nézeteit idővel felülvizsgálta, és elfogadta, hogy „egy jogi norma érvényességéhez nem elegendő az, hogy egy egyébként többé-kevésbé hatásos jogrendhez tartozzék, hanem magának a jogi normának is bizonyos mértékben hatásosnak kell lennie".[129]

Visegrády különbséget tesz a jogi és a társadalmi hatékonyság között. Az előbbi a formális jogkövetésre, az utóbbi az elérni kívánt társadalmi cél megvalósulására utal. Arra is keresem a választ, hogy a Rendelet által megteremtett védelem milyen módon tehető hatékonyabbá a jövőben, az általunk jelenleg ismert feltételek ismeretében. Ezzel azt is állítom természetesen, hogy a Rendelet nem az elérhető legmagasabb szintű védelmet biztosítja. A magánszféra védelmét hatékonyabban szolgáló norma- és intézményrendszer is létrehozható. E feltételezés nélkül a védelmi lépcső elméletének elemzése nem vezetne eredményre.

A Rendelet maga is számos ponton utal a Rendelet szabályainak hatékony érvényesítésére. Mintha ebben is tetten érhető lenne az a különbségtétel, amit Visegrády is megfogalmazott a jogi és társadalmi hatékonyság között, továbbá Giovanni Buttarelli híressé vált mondása, amely szerint „számomra a jognak való megfelelés nem elegendő", utalva a jog formális teljesítésén túlmutató többletkövetelményekre.[130]

A Rendelet nagyon sok helyen használja a hatékony kifejezést, így többek között:
- a személyes adatok hatékony védelméről beszél (11),
- az adatkezelőnek megfelelő és hatékony intézkedéseket kell végrehajtania (74),
- a magatartási kódexek kapcsán a hatékony alkalmazás elősegítését mint jogalkotói célt említi (98).
- A tagállami adatvédelmi hatóságokat is fel kell ruházni a hatékony feladatellátáshoz szükséges eszközökkel (120),
- továbbá e felügyeleti hatóságok döntéseinek hatékony végrehajtása szintén jogalkotói cél (127).

[129] Szilágyi Péter az idézett műben Hans Kelsen *Tiszta jogtan* című munkáját idézi Bibó István fordításában (Budapest, ELTE Bibó István Szakkollégium, 1988).

[130] A híres beszéd Giovanni Buttarelli halála előtt tíz hónappal, az International Conference of Data Protection and Privacy Commissioners (ICDPPC) 2018-as konferenciáján hangzott el Brüsszelben, 2018 októberében: „[…] for me, compliance with the law is not enough". A videó elérhető a YouTube oldalán.

– A felügyeleti hatóságok döntéseivel szemben szintén hatékony jogorvoslatot kell biztosítani az érintettek számára (143).
– A felügyeleti hatóság által kiszabható büntetéseknek is, többek között a hatékonyság kritériumának is meg kell felelnie (152).
– Az adatkezelő kötelezettségei között rögzíti a Rendelet, hogy az adatkezelés biztonságát szolgáló intézkedéseknek hatékonynak kell lenniük (32. cikk [1] d) pont).

Végül az Európai Bizottság a Rendelet szabályainak értékelése és felülvizsgálata során azok alkalmazását és hatékonyságát vizsgálja (97. cikk [2] bekezdés).

Az adatvédelmi hatóságok hatékony működése

A személyes adatok védelméhez fűződő jog érvényesülése, a jog hatékonysága körében az adatvédelmi felügyeleti hatóság működésének hatékonysága is vizsgálandó. A hatóság feladat- és hatáskörének vizsgálatakor, a védelmi lépcső elméletének alkalmazása során nem tekinthetünk el attól, hogy a hatóság hatékony működését egy minimális elvárásként fogalmazzuk meg. A hatóság a rendelkezésére álló anyagi és szellemi forrásokkal felelősen kell hogy gazdálkodjon. Ennek mércéje nem csupán gazdasági természetű, hanem kifejezetten a társadalmi hatékonyság. Kritikus megközelítést alkalmazok akkor, amikor a hatóság számára elkülönített költségvetést a magánszféra állapotának fényében vizsgálom. Nem a Rendelet, a jelenlegi állapot a mérce, hanem az elérhető legmagasabb szintű védelem foka. A hatóságoknak készen kell állniuk arra, hogy az alakuló igényekhez alkalmazkodni tudjanak.

Feltételezésem szerint azonos jogi szabályozás mellett is jelentős eltéréseket mutathat egyes országok között az adatvédelem szintje és az adatvédelmi kultúra állapota. Azt állítom tehát, hogy önmagában az általános adatvédelmi Rendelet, mint az EU valamennyi tagállamában közvetlenül alkalmazandó jogalkotási aktus, nem garantálja az azonos védelmi szintet. Ennek oka nemcsak az eltérő jogi hagyományokban és ágazati szabályokban keresendő, hanem abban is, hogy a Rendelet maga enged sok helyen eltérést a tagállami jogalkotó számára. A részletes elemzés, a védelmi lépcső elméletének alkalmazása révén minden bizonnyal jelentős különbségeket fedezhetünk fel tagállam és tagállam között. Nem véletlen, hogy az elemzés kifejezetten a mikroszintre is fókuszál, erre szolgál az adatvédelmi tiszt-

viselők szerepét bemutató fejezet. Sok kérdés eldől az adatkezelő szervezeten belül, a védelem erősítése nagyban múlhat a jól működő adatvédelmi tisztviselő tevékenységén.

A szabályozás vizsgálata nem elegendő ahhoz, hogy megállapítsuk a védelem minőségét. Ezért is szükséges a gyakorlati körülmények vizsgálata. Az adatvédelem nem csupán a szabályozáson múlik, hanem döntések sorozatán, az adatkezelő szervezetén belül az adatkezeléseket érintően, vagy éppen hatósági és bírósági döntéseken áll. Ezért is van különleges jelentősége, hogy a jövőbe tekintve felvázoljunk egy olyan állapotot, ahol a védelem erősebb, mint a jelenleg tapasztalt. Ez minden esetben az a harmadik fok, ahova érdemes lenne továbblépni, ahol a jog hatékonyabban szolgálja a jogalkotói célt, témánk körében a magánszféra védelmét.

Vákát

A védelem komponensei – a védelmi lépcső révén mérhető indikátorok általános elemzése

Ebben a fejezetben számba veszem azokat az összetevőket, amelyekre a védelmi lépcső elméletét alkalmazandónak tartom. Megjelölöm azokat az aspektusokat, amelyek révén ezeknek a komponenseknek a minősége meghatározható, és azt is, hogy miként hatnak összességében a védelem szintjére. Az egyes komponenseknél azonosítom a jelenlegi szintet, amely a Rendelet szabályozására utal, a korábbit, ami általában az irányelvi szabályozásra mutat vissza, és ahol releváns, megemlítem azt a kívánatos szintet, amely előrelépést jelentene a jelenlegi szinthez képest.

A Rendelet hatálya

A jogszabály hatálya értelemszerűen jelentős szerepet játszik az általa nyújtani kívánt védelem tekintetében. A hatály meghatározásakor eldől, hogy bizonyos adatok, magatartások, ügyek, illetve személyek esetében a védelem már nem érvényesül.[131]

> A jogalkotó például az elhunyt személyekre nem terjesztette ki a Rendelet által nyújtott védelmet. A (27) preambulumbekezdés szerint: „Ezt a Rendelet[et] nem kell alkalmazni az elhunyt személyekkel kapcsolatos személyes adatokra. A tagállamok számára lehetővé kell tenni, hogy az elhunyt személyek személyes adatainak kezelését szabályozzák."

Tekintettel arra, hogy az EU-ban létezett már átfogó adatvédelmi szabályozás az 1995-ben elfogadott adatvédelmi irányelv révén, ezért a hatályt illetően csupán a korábbi szabályozáshoz, a 95/46/EK irányelvhez képest mutatkozó kockázatot, valamint a Rendelet e tekintetben jelentős és védelmet erősítő újítását említem.

[131] E mozgástérrel élt a magyar törvényalkotó, amikor az Infotv. 25. §-ában az adatok halál esetére szóló rendelkezés szabályait rögzítette.

Tárgyi hatály

A Rendelet tárgyi hatálya kiterjed minden olyan műveletre, amelyet személyes adatokon hajtanak végre. A személyes adat fogalmával kapcsolatban jelentős bizonytalanságok nem merültek fel, a 29. cikk szerinti adatvédelmi munkacsoporti jogértelmezés például a határesetekre nézve jól követhető iránymutatást kínál. Szemléltetésül: a 29. cikk alapján létrehozott Adatvédelmi Munkacsoport 4/2007. számú véleménye kiegyensúlyozott megközelítést alkalmaz, kerüli az adatvédelmi szabályok hatályának túlfeszítését, de az indokolatlan korlátozást is.[132]

Az adatkezelésre vonatkozó szabályok hatálya több problémát is felvet.

A tárgyi hatályra vonatkozó szabály szerint a nem automatizált módon történő adatkezelésre akkor kell alkalmazni a Rendeletet, amikor az adatok „valamely nyilvántartási rendszer részét képezik, vagy amelyeket egy nyilvántartási rendszer részévé kívánnak tenni".[133] A hatály ilyen szűkítése felveti a papíralapú dokumentumokban található adatok védelmének lehetséges csökkenését. Kijátszhatónak tűnik a szabály, különös tekintettel arra, hogy azok az iratok, amelyek „nem rendszerezettek meghatározott szempontok szerint", kívül esnek a Rendelet hatályán és az abban található adatok védelme nem biztosított.[134] A 95/46/EK irányelv tartalmában azonos módon szabályozott, azonban irányelv lévén, elsődlegesen a tagállami átültetése érvényesült.

Jelentős kockázatként kell számontartanunk ezt a szabályt, amely a 95/46/EK irányelv magyarországi átültetéséhez képest visszalépést jelent. A közvetlenül alkalmazandó uniós szabály ellenében a hazai jogalkotó meg tudja teremteni annak lehetőségét, hogy ez a visszalépés kiküszöbölhető legyen, ahogyan az Európa Tanács úgynevezett 108-as egyezménye kapcsán is megtörtént ez.

> Az Európa Tanács egyezménye az egyének védelméről a személyes adatok gépi feldolgozása során (az úgynevezett 108-as egyezmény) 3. cikkében a hatályt illetően úgy fogalmaz, hogy bármely állam nyilatkozatot tehet arról, hogy „a jelen egyezményt alkalmazza a személyes adatok nem gépi eszközökkel feldolgozott

[132] Az Európai Bizottság (a 29. cikk szerinti Munkacsoport titkárságának) honlapja. *Edpb.europa.eu*.

[133] A Rendelet 2. cikk (1) bekezdése szerint.

[134] A Rendelet (15) preambulumbekezdése szerint.

állományaira is". Ilyen módon a magyar jogalkotó kiterjeszthette az egyezmény hatályát olyan adatokra is, amelyek egyébként nem esnének a Rendelet alkalmazási körébe. Erre sor is került, az egyezményt inkorporáló 1998. évi VI. törvény 3. §-a rögzíti, hogy „[a] Magyar Köztársaság Kormánya kijelenti, hogy az Egyezmény 3. Cikke 2. c) pontja alapján az Egyezményben foglaltakat alkalmazza a személyes adatok nem gépi eszközökkel feldolgozott állományaira is". Magyarország az Európa Tanács Egyezménye tekintetében tehát a kiterjesztett védelem mellett döntött, hasonló deklarációra a Rendelet esetében azonban nincs lehetőség. Az unió tagállamainak egy része tett, egy része pedig nem tett a magyarhoz hasonló deklarációt, tehát a 108-as egyezmény átültetése sem teljesen egységes az Európai Unióban. Hozzá kell tennünk, hogy a tárgyi hatály e különbsége feltételezhetően ritkán fogja érinteni a személyes adatok szabad áramlását, hiszen itt olyan, adott esetben nem tipikusan strukturált adatokról van szó, amelyeket jellemzően nem szoktak a napi üzletmenet során rutinszerűen továbbítani. Ettől függetlenül a védelmi szint sajnálatos csorbulásáról van szó a nem géppel feldolgozott adatok esetében.

Magyarország kifejezetten vállalta, hogy az Egyezményt az adatok nem géppel feldolgozott állományaira is alkalmazni fogja. Hasonló vállalás ugyan nem tehető a Rendelet kapcsán, de annak nincs akadálya, hogy a hazai jogalkotás kiterjessze a védelmet a nem automatizált adatkezelésekre. (Vizsgálatom pusztán az Európai Unió jogának elemzésére irányul. Következetlenségnek tűnhet, hogy a tárgyi hatály kapcsán mégis tagállami jogi példát hozok fel. Azért tartottam szükségesnek ezt a témát az elemzés általános irányától függetlenül mégis felvetni, mert olyan súlyú kockázatnak tekintem, amelynek kapcsán a tagállami korrekciós lehetőség mindenképpen megemlítendő a védelmi szint elemzése során.) A magyar adatvédelmi hatóság gyakorlata igazolta, hogy a védelem a papíralapú dokumentumokra is kiterjesztendő.

A Nemzeti Adatvédelmi és Információszabadság Hatóság a NAIH/2017/148-as számú, a Magyarországi Szcientológia Egyház adatkezelése ügyében folytatott hatósági eljárásában például javarészt papíralapú dokumentumokat és a papíralapú dokumentumokban megvalósuló adatkezelést vizsgálta. A munkatársi akták, az úgynevezett PC *(pre-clear)* dossziék, az etikai dossziék és a leveleződossziék az egyház napi működéséhez tartoztak. Az iratok és dossziék rendezettsége, rendszerezettsége, kereshetősége révén az irányelv tárgyi hatálya alá tartoztak. Mindazonáltal ez a vizsgálat is rámutatott arra, hogy a legsúlyosabb

jogsértések nem feltétlenül és kizárólag elektronikus úton valósulhatnak meg. A 21. században is találkozni lehet papíralapú adatkezelésekkel, és súlyos jogalkotói mulasztás lenne, ha a tárgyi hatály szűkítése révén ezek az adatkezelések kívül esnének az adatvédelem hatályán általában. A súlyos személyiségi jogi jogsértések is indokolják az adatvédelmi szabályok alkalmazandóságát, és alátámasztják az adatvédelmi felügyeleti hatóságok hatásköreinek gyakorolhatóságát. A NAIH említett határozatát a Fővárosi Törvényszék 13.K.700.014/2018/60. számú ítélete révén, a felülvizsgálati eljárás során hatályában fenntartotta. Ami a NAIH határozat tárgyi hatályát illeti, a Törvényszék is rámutatott arra, hogy „a felpereseknek a strukturálatlanságra vonatkozó állítása alaptalan, mert a PC dossziék, az Etikai dossziék, a Munkatársi dossziék, és a Tanulói dossziék tartalma strukturált adatállományt takar. Az érintettekről gyűjtött adatok aktatípusonként rendszerezve vannak; azokat külön helyiségben, ABC sorrendben tárolják; a dossziékon belül időrendi elhelyezést alkalmaznak; az összefoglaló dokumentumok is elősegítik az aktában történő keresést; az érintettek által adott hozzájárulásokat külön aktában, ABC rendben, lefűzve tartják nyilván, mely szintén biztosítja a személyes adatok kereshetőségét." A törvényszéki ítélet ilyen módon kifejtette, hogy a bírói mérlegelés körében milyen kritériumokat vesz figyelembe akkor, amikor a tárgyi hatályra vonatkozó szabályok érvényesülését vizsgálja.

A védelmi lépcső alkalmazásával azt kell kimondani, hogy az adathordozótól független védelem jelenti a magasabb védelmi szintet, amelyhez képest visszalépés az Európai Unió olyan szabályozása, amely az egyik adathordozót, nevezetesen a hagyományos, papíralapú dokumentumokban tárolt személyes adatok jelentős részét kivonja a tárgyi hatály alól.

A Kúria mint felülvizsgálati bíróság a Kfv.III.37.911/2017/8. számú ügyben hozott ítéletében a Budapest Főváros Levéltára által folytatott adatkezelést vizsgálta. Az ügyben vizsgált tényállás szerint egy kutató beiratkozott a szóban forgó közlevéltárba, és „korabeli bűnügy" kutatási tárgyat jelölt meg. A kutatási kérelemben megjelölte azokat a személyeket, akiket egy konkrét büntetőügyben elítéltek egy adott évben. Ennek alapján jutott olyan információkhoz a kutató, amelyeket aztán később az interneten közzétettek, és súlyosan befolyásolták az érintettek helyzetét, társadalmi megítélését. A papíralapú adatkezelések tehát jelentős mértékben határozhatják meg az egyének társadalmi boldogulásának esélyeit, különösen például köziratokban tárolt információk újbóli publikációja

révén. A vizsgált esetben a Kúria, a NAIH határozatával egyetértve, jogsértőnek minősítette a személyes adatok védelmi idő lejárta előtti, levéltár általi kiadását.

Az Európa Tanács együttműködésében tett magyar vállalás, amely szerint az adathordozótól függetlenül nyújtandó a védelem, magasabb szintű védelmet eredményez. Ez tehát az a szint, amely megőrzendő, mind az irányelvi, mind a rendeleti szabályozás ehhez képest alacsonyabb védelmi szintet jelent.[135]

Területi hatály

A Rendelet újítása az úgynevezett irányultsági szabály, amely figyelembe veszi a célpiacon élő személyek magánszférájának védelmét. A területi hatály kiterjesztése révén nem csupán az olyan adatkezelésekre kell alkalmazni a Rendeletet, amelyek az Európai Unió területén történnek, hanem azokra is, amelyek azon kívüliek és az Unióban tartózkodó érintettek adatainak kezelésével járnak. Az irányultsági szabály szerint az extraterritoriális hatály azokra az adatkezelésekre terjed ki, amelyek áruk vagy szolgáltatások nyújtásához kapcsolódnak, továbbá az érintettek unión belül tanúsított viselkedésének megfigyelésével függenek össze.[136] A védelem szintjét egyértelműen erősítő újítása ez a Rendeletnek, hiszen a területi hatály kiterjesztése növeli azon vállalkozások és adatkezelések számát, ahol a Rendelet által elvárt magas szintű védelem érvényesítendő.

Az adatvédelmi szabályok érvényesítésének kiterjesztésében versenyjogi megfontolások is megjelenhetnek kisegítő jelleggel. Az Európai Unió Bíróságának ítélete a Google ügyében[137] alkalmazza a kétoldalú piacok elméletét. Bár a Bíróság

[135] Nem állítok újat, amikor a főszabállyá váló digitális alapú adatkezelések időszakában az offline védelem fontosságát hangsúlyozom. Az ENSZ 2014. január 21-ei, *The Right to Privacy in the Digital Age* című közleménye a 3. pontjában megerősíti, hogy online és offline közegben ugyanazok a jogok biztosítandók („[…] the same rights that people have offline must also be protected online, including the right to privacy"). Forrás: az ENSZ honlapja.

[136] A Rendelet 3. cikkének (2) bekezdése szerint a területi hatály az ingyenes áruk vagy szolgáltatások nyújtásához kapcsolódó adatkezelésekre is kiterjed.

[137] C-131/12. sz. Google Spain SL és Google Inc. kontra Agencia Española de Protección de Datos (AEPD), Mario Costeja González ügyben 2014. május 13-án hozott ítélet (EU:C:2014:317).

sehol nem nevesíti, alkalmazza ezt az elvet. Amennyiben ugyanis a kétoldalú piac valamelyik oldala, a Google esetében a profitot termelő oldal az unió jogának hatálya alá esik, úgy a profitot nem termelő oldal sem vonható ki az uniós jog hatálya alól. Ez az érvelés is a hatály kiterjesztésének irányába mutat, amint arról az adatkezelő fogalmának széles körű alkalmazása kapcsán is szólok.[138]

Az adatvédelmi irányelv e tekintetben egyértelműen a védelmi lépcső alacsonyabb szintjén állt, amelyhez képest a Rendelet az extraterritoriális hatály bevezetésével magasabb szintre lépett.

A védelem hatósági kikényszerítési lehetőségét is figyelembe véve az jelentene előrelépést a jelenlegi, rendeleti szabályozáshoz képest, ha a tagállami adatvédelmi hatóságok harmadik országbeli adatkezelőkkel szembeni eljárása összehangolt módon valósulhatna meg. Ez gyakorlatilag nem szabályozási feladat, hanem az adatvédelmi hatóságok együttműködésének területére tartozik, mindazonáltal a Rendelet egységes alkalmazása és kikényszerítése terén az érintetti jogok és általában az adatvédelmi követelmények hatékonyabb érvényesítését eredményezhetné. Ennek megvalósulásához a harmadik országokkal való együttműködés is előfeltétel, ezen a téren az unió még nem élt minden rendelkezésre álló eszközzel. Az előrelépés lehetősége tehát gyakorlati szinten is megfogalmazható.

Személyi hatály

A személyi hatály terén a Rendelet nem változtatott a korábbi, Európában általános megközelítésen, amely szerint az alapjogokat mindenki számára, állampolgárságtól függetlenül biztosítják a tagállamok, illetve az Európai Unió intézményei. Ez egy olyan ambíció, amely egyértelműen az erős védelem irányába mutat. Az Amerikai Egyesült Államok szabályozása más kiindulópontokon nyugszik. Részben ebből is fakad az a konfliktus, amely a harmadik országba irányuló adattovábbítás feltételei kapcsán végigkíséri a két partner szabályozásának viszonyát. Az Európai Unió és az Amerikai Egyesült Államok szabályozása között több különbség is mutatkozik. Így

[138] Vö. Szabó Endre Győző: A kétoldalú piacok elmélete és a személyes adatok védelme – a Google-ítélet elemzése versenyjogi és adatvédelmi szempontok szerint. *In Medias Res,* 6. (2017), 1. 170–181.

például az amerikai jogrendszerben nincsen általános adatvédelmi keretnorma, ezért alapvetően szektorális szabályokra épül az adatvédelem.[139]

A hatály kérdését nem csupán a jogszabály, hanem a kapcsolódó joggyakorlat alapján is lehet elemezni. Az Európai Unió Bírósága az adatvédelmi ügyek megítélése során tekintettel van arra a jogalkotói célra, hogy az adatok magas szintű védelmét kívánja garantálni. A Bíróság elemzése szerint a Rendelet szélesen határozza meg az adatkezelő fogalmát, és e rendelkezés arra irányul, hogy az érintetteknek hatékony és teljes védelmet biztosítson. A Bíróság tehát a saját értelmezési keretei között is érvényt kíván szerezni a hatály terén adódó mérlegelés során a jogalkotói célnak, és a védelem magas szintjének biztosítását kívánja elősegíteni.[140] E tendenciába illeszkedik a Bíróságnak az az ítélete, amely szerint a közösségi oldal rajongói oldalának *(fan page)* adminisztrátora társadatkezelőnek tekintendő, illetve a közösségi oldal modulját a saját honlapján megjelenítő, és ezáltal többlet-adatkezelést lehetővé tevő honlap fenntartó adatkezelői felelőssége is megállapítható.[141]

[139] Vö. Péterfalvi Attila (szerk.): *Adatvédelem és információszabadság a mindennapokban*. Budapest, HVG-ORAC, 2012. 25–28.

[140] A Bíróság gyakorlatában több helyen felmerül ez a szempont, így például az Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein versus Wirtschaftsakademie Schleswig-Holstein-ügyben hozott előzetes döntésben, C-210/16. számú ügyben, 27–28. pont. ECLI:EU:C:2018:388. Hasonlóan: 2014. május 13-i Google Spain és Google ítélet, C-131/12, EU:C:2014:2428.

[141] Az Európai Unió Bíróságának C-40/17-es számú, 2019. július 29-én a Fashion ID GmbH Co. KG és a Verbraucherzentrale NRWeV közötti ügyben hozott ítélete (A Bíróság ítélete [második tanács], 2019. július 29. Fashion ID GmbH & Co.KG kontra Verbraucherzentrale NRW eV, ECLI:EU:C:2019:629) szerint a honlapon a „Like" modul beépítése nélkül nem kerülne sor adattovábbításra a Facebook számára. Az kétségtelen, hogy a Fashion ID nem tehető felelőssé azokért az adatkezelésekért, amelyeket a továbbítást követően a Facebook végez az így megszerzett személyes adatokon. Az adatok gyűjtése tekintetében ugyanakkor a Facebook és a Fashion ID közösen határozzák meg az adatkezelés célját és módját. A Bíróság érvelése szerint tehát a honlapon ilyen modult elhelyező fenntartó nem mentesülhet az adatkezelői felelősség alól, ami a Wirtschaftsakademie ítélethez hasonlóan az adatkezelő fogalmának kiterjesztő értelmezésére, ilyen módon pedig a védelem hatályának kiterjesztésére irányul.

Az Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein és Wirtschaftsakademie Schleswig-Holstein közötti ügyben hozott előzetes döntésben a Bíróság kimondta, hogy az egyszerű felhasználó nem válik a Facebookkal együtt felelőssé a személyes adatok kezeléséért, azonban a rajongói oldal adminisztrátora nem egyszerű felhasználó. Ami a különbségtételt indokolja, az az, hogy a rajongói oldal létrehozója lehetővé teszi a Facebook számára, hogy az oldal látogatóinak számítógépén cookie-kat helyezzen el, függetlenül attól, hogy a felhasználó egyébként a Facebooknak is felhasználója (35. pont). Az utóbbi személyi kör vonatkozásában az adminisztrátor felelőssége fokozottabb (41. pont). Az adminisztrátornak beállításokat kell eszközölnie az oldalon, ami befolyásolja a személyes adatok kezelését. A célközönségre vonatkozóan számos beállítást megtehet, így kor, nem, családi állapot, szakmai helyzet, demográfiai adatok, életmód, érdeklődési kör, online vásárlási szokások, a felhasználót érdeklő termékek vagy szolgáltatások kategóriái, földrajzi adatok tekintetében (37. pont). Összességében tehát az adminisztrátor részt vesz a személyes adatok kezelése céljának és módjának meghatározásában, tehát ő is adatkezelőnek tekintendő (39. pont). Ez az ítélet is példa az adatkezelői minőség minél szélesebb alkalmazására.

A védelmi lépcső legmagasabb fokaként határozhatjuk meg a Rendelet azon megközelítését, hogy a védelem az általános személyi hatály révén minden megkülönböztetés nélkül kiterjed minden olyan személyre, adatalanyra, akinek személyes adatait az EGT valamely tagállamának joga alá tartozó adatkezelő kezeli.

Az adatkezelői, illetve adatfeldolgozói felelősség terén a Rendeletre épülő joggyakorlat álláspontunk szerint az erősödő védelem irányába mutat. A védelmi lépcsőn előrelépésként értékeljük, ha a szabályok érvényesülése javul. A bírói gyakorlat alakulása megerősíti, hogy az irányelvi szabályozáshoz képest előrelépést tudunk megállapítani. Itt a bíráskodásnak azzal a szerepével szembesülünk, hogy képes egyedi döntések révén megerősíteni a védelmet: iránymutatást és jogbiztonságot nyújt a jogalkalmazásban. Elejét veszi annak, hogy a jogbizonytalanság révén a védelem eróziónak induljon. Az előzetes döntéshozatal rendszerének a védelem megőrzése szempontjából tehát kiemelt szerep jut.

A lehetséges előrelépés szintjének meghatározását a személyi hatály kapcsán nem tartom időszerűnek, ennek mérlegeléséhez a Rendelet alkalmazása során nyert hosszabb tapasztalatra van szükség.

Definíciók

A fogalommeghatározások is alkalmasak lehetnek a védelmi szint alakítására. Egyrészt módot nyújtanak arra, hogy olyan személyekre, adatokra, tevékenységekre terjesszék ki a védelmet, akik és amelyek korábban nem estek az alá, továbbá az adatvédelmi szabályozás magasabb szintű védelme körébe sorolhat át bizonyos magatartásokat, illetve adatokat.

Ez utóbbira példa a Rendeletben a „természetes személyek egyedi azonosítását célzó"[142] genetikai és a biometrikus adatok átsorolása a személyes adatok különleges kategóriájába. Korábban, az irányelvi szabályozás idején ezek az adatok a „közönséges" személyes adatok körébe tartoztak az uniós szabályok szintjén. Ezt a kiterjesztést már évekkel a jogalkotás előtt szorgalmazták, többek között a European Group on Ethics in Science and New Technologies to the European Union.[143] Az átsorolás uniós szintű egységesítése révén a genetikai és biometrikus adatok alanyai igényt tarthatnak a különleges kategóriába tartozó adatoknak járó fokozott védelemre. Ez a magasabb védelem az adatkezelés jogalapjának szigorúbb szabályaiban mutatkozik meg, illetve abban, hogy a személyes adatok különleges kategóriáit célzó automatizált döntéshozatal és profilalkotás csak bizonyos meghatározott feltételek mellett engedélyezhető.

A védelem további elemei is társulnak még a definíciós átsoroláshoz, így szigorúbb szabályok vonatkoznak:
- az unióban letelepedési hellyel nem rendelkező adatkezelő képviselőjének kijelölésére;
- az adatvédelmi hatásvizsgálat kapcsán is magasabb kockázatot jelent a különleges adatok kezelése;
- a különleges adatok nagy számban történő kezelése adatvédelmi tisztviselői kinevezés kötelezettségével jár;
- az adatgyűjtés céljától eltérő célú adatkezelés mérlegelése során tekintettel kell lenni a különleges adatokra, illetve az általuk védett kiemelt érdekekre;

[142] A Rendelet 9. cikk (1) bekezdésének fordulata szerint.

[143] European Commission, European Group on Ethics in Science and New Technologies: *Ethics of Information and Communication Technologies.* Publications Office, 2012. Opinion No. 26. 61.

– a belső nyilvántartási kötelezettség alóli mentesülés lehetősége korlátozott, ha az adatkezelő különleges adatokat is kezel;
– a kötelező erejű vállalati szabályok között külön rögzíteni kell a különleges adatok kezelésének feltételeit.

Mindezen adatok, illetve az adatok alanyai tekintetében megállapíthatjuk, hogy a védelem a kedvező irányba, magasabb szintre lépett a korábbi, irányelvi időszakhoz képest.

A lehetséges előrelépésről az egyes definíciók részletesebb vizsgálata révén lenne lehetőség. E helyütt az elmondottakra szorítkozunk, tudva, hogy a definíciók és a védelmi szint elemzése részletesebb elemzés tárgyát képezhetné.

Átláthatóság

Az átláthatóság a Rendelet egyik alapelve. Az elv célja annak biztosítása, hogy az érintett számára követhető legyen az adatkezelési műveletek összessége az adatok gyűjtésétől kezdve, azok felhasználásán át, adott esetben azok törléséig. Az érintett számára ismertnek kell lennie, hogy ki az adat kezelője, kik kapnak az adatokhoz hozzáférést, milyen jogai vannak, és ezekkel hogyan élhet.[144]

Az átláthatóság következetes érvényesítése, illetve kiterjesztése erősíti a védelmet, hiszen az érintett számára követhetővé válik az adat útja, ilyen módon lehetősége nyílik információs önrendelkezési jogának gyakorlására, például a hozzájárulás visszavonására, az adatok helyesbítésére, vagy adott esetben jogorvoslat igénybevételére. A transzparencia elősegítésének jogalkotói szándéka a Rendelet több rendelkezésében és új jogintézményében is megmutatkozik.

Az érintettnek nyújtandó tájékoztatásra és kommunikációra vonatkozó szabályok uniós szintű egységesítése önmagában is előrelépésnek tekinthető a védelem terén. Az előző lépcsőfoknak az irányelvi szabályozás idején a széttöredezett szabályozás, következetlen elvárásrendszer volt a jellemzője.

[144] Az átláthatóság elvének részletes tartalmát a Rendelet (39) preambulumbekezdése írja le.

A profilalkotás és az automatizált egyedi döntéshozatal esetében az érintett élhet a tiltakozás jogával, erről pedig őt előzetesen tájékoztatni kell. Az érintetti jog gyakorlását szolgálja az átláthatóság kiterjesztése ezekre az esetekre.[145]

A személyes adatok biztonságát fenyegető véletlen vagy jogellenes módon kialakult adatvédelmi incidens esetében kötelező bejelentést tenni az adatvédelmi felügyeleti hatóságnak, továbbá az érintettet is tájékoztatni kell, ha az valószínűsíthetően magas kockázattal jár az adatalanyok jogaira nézve.[146] Ilyenkor az érintetteket „késedelem nélkül" tájékoztatni kell az incidensről. Az átláthatóságot szolgáló szabály lehetővé teszi, hogy az érintett maga is megtehesse azokat az intézkedéseket, amelyek saját jogai és érdekei védelmében szükségesek.[147]

Szintén az átláthatóságot erősíti az adatvédelmi tisztviselő működése, akihez az érintett a jogai gyakorlásához kapcsolódó valamennyi kérdésben fordulhat.[148]

Az elszámoltathatóság elve átível az elvek és szabályok rendszerén. Az elv azt az elvárást fogalmazza meg, hogy az adatkezelő feleljen meg a jogszabályoknak, és ezt erre irányuló kérés esetén be is tudja mutatni.[149]

Az átláthatóság elvének rögzítése a Rendeletben az elvet szolgáló további intézményekkel kiegészítve jelentősen javítják a védelem esélyét és lehetőségét. A védelem erősítése érdekében szükséges az érintettek bevonása valamilyen formában a döntések előkészítésébe. Az átláthatóság ilyen megerősítésének a következő, mielőbb elérendő védelmi fok a jellemzője. Az irányelvi szabályokhoz képest, amelyek a transzparencia terén az említett esetekben nem fogalmaztak meg ilyen egyértelmű kötelezettségeket, a rendeleti szabályozás a védelmi lépcső magasabb fokát jelenti.

Az előrelépés lehetőségéről a későbbi fejezetekben szólok részletesen, különösen az adatvédelmi tisztviselő és a felügyeleti hatóság együttműködése kontextusában.

[145] A tiltakozáshoz való jogot a Rendelet 4. szakasza, 21. és 22. cikke szabályozza.

[146] Az érintett tájékoztatására az adatvédelmi felügyeleti hatóság is kötelezheti az adatkezelőt a Rendelet 58. cikk (2) bekezdés e) pontja szerint.

[147] Az adatvédelmi incidensre vonatkozó szabályokat a Rendelet 33. és 34. cikke írja elő, és ide kapcsolódik a 4. cikk 12. pontja az incidens fogalommeghatározása révén.

[148] A Rendelet 38. cikk (4) bekezdése szerint.

[149] A Rendelet 5. cikk (2) bekezdése szerint.

Az érintettek jogai

A Rendelet nem csupán megerősíti a korábbi szabályozásban már biztosított érintetti jogokat, hanem újakat is bevezet. Az érintetti jogok bővülése az irányelvi katalógushoz képest látványos előrelépést jelent a védelmi lépcsőn.

A törléshez *(right to erasure),* illetve elfeledtetéshez való jog tartalma részben új, amennyiben az adatok online környezetben való nyilvánosságra kerülése esetén az adatkezelő köteles minden észszerű lépést megtenni annak érdekében, hogy mindazokat az adatkezelőket tájékoztassa a törlés iránti igényről, akik szintén kezelik az adatokat. A törlés, illetve elfeledtetés jogának részletes szabályait a Rendelet 17. cikke rögzíti. Az online közegben nemcsak az adatok törlése, hanem bizonyos linkek eltávolítása is kötelezettségként jelenik meg. A bírói jogfejlesztés – és nem a Rendelet – újítása a keresőmotorok találati listájából egyes linkek eltávolításának igénye. Ez utóbbit is szokás az elfeledtetéshez való jogként *(right to be forgotten)* említeni.[150]

Az adathordozhatósághoz való jog *(right to data portability)* a Rendelet újítása. Bár ezt a jogot valóban a Rendelet vezette be, a kodifikálásra való igény az Eurobarometer 2010-es és 2015-ös kutatásában is felmerült, és 2010-ben, majd 2015-ben is a megkérdezettek kétharmada fontosnak tartotta, hogy az adatait a régi szolgáltatótól az új szolgáltatóhoz át tudja vinni.[151] A jog lényege, hogy bizonyos feltételek fennállása esetén az érintett kérheti, hogy a saját maga által rendelkezésre bocsátott adatokat géppel olvasható formátumban megkapja az adatkezelőtől, vagy kérelmezheti az adatok általa megjelölt adatkezelőhöz való továbbítását.[152]

A 29. cikk szerinti Munkacsoport iránymutatása az érintett által „rendelkezésre bocsátott" kitétel széles értelmezését javasolja. Figyelemre méltó az iránymutatás

[150] Az Európai Unió Bíróságának ítélete a Google Spain SL és Google Inc. versus Agencia Española de Protección de Datos (AEPD), Mario Costeja González ügyben, C-131/12.sz. ECLI:EU:C:2014:317.

[151] Special Eurobarometer Report (431) – Data Protection (Adatvédelem). *Europa.eu/eurobarometer,* 2015. 42–43. In Special Eurobarometer Report (359) – Attitudes on Data Protection and Electronic Identity in the European Union (Az adatvédelemmel és az elektronikus személyazonossággal kapcsolatos hozzáállás az Európai Unióban). *Europa.eu/eurobarometer,* 2011. 160–162.

[152] A jog tartalmát a Rendelet 20. cikke szabályozza.

azon megjegyzése is, amely szerint az adathordozhatóság joga „fontos eszköz, ami elő fogja segíteni az adatok szabad áramlását az EU-ban és támogatni fogja az adatkezelők közötti versenyt”.[153]

A piaci verseny elősegítése mellett a jog célja az is, hogy hatékonyabbá váljon az érintett rendelkezési joga az adatai felett.[154] E jog gyakorlati érvényesülésével kapcsolatban számos kétely felmerült, a jog szabályozása továbbfejlesztést igényel, amely szerepel is az Európai Bizottság Európai adatstratégia című dokumentumában.[155] A dokumentum a 23–25. oldalán a kulcsintézkedések között említi az adathordozhatósághoz való jog megerősítésének lehetőségeit. A módosítás célja az, hogy nagyobb ellenőrzési lehetőség álljon az érintettek rendelkezésére abban a tekintetben, hogy ki férhet hozzá a gépi úton előállított adatokhoz, és ki használhatja fel azokat.

Az érintetti jogok katalógusának bővülése mindenképpen a védelem erősítését szolgálja. Amint látni fogjuk, a jog kikényszerítésének eszközei is bővülnek, és ez azt vetíti előre, hogy az érintettek valóban tudnak majd élni az új jogosultságokkal.

A „González kontra Google”-ügy kapcsán, a listáról való eltávolítás ügyében első körben a keresőmotor üzemeltetőjéhez fordul az érintett, majd, ha elégedetlen a válasszal, illetve az intézkedéssel, akkor megnyílik a lehetősége annak, hogy az adatvédelmi hatósághoz vagy a bírósághoz forduljon. A Google európai országokban letelepedett, az adatkezelésben is szerepet vállaló leányvállalatai révén az EU joga is alkalmazandóvá válik, és így megnyílik a jogérvényesítés uniós, illetve tagállami szabályai szerinti lehetősége.[156]

[153] *Article 29 Data Protection Working Party, Guidelines on the Right to Data Portability, WP 242.* 3. és 8–9. Forrás: az Európai Bizottság (a 29. cikk szerinti Munkacsoport titkárságának) honlapja.

[154] A felhasználócentrikus megközelítés és az interoperabilitás kapcsolatáról bővebben lásd például: Paul De Hert et al.: The Right to Data Portability in the GDPR: Towards User-centric Interoperability of Digital Services. *Computer Law & Security Review,* 34. (2018), 2. 193–203.

[155] Európai Bizottság: *A Bizottság közleménye az Európai Parlamentnek, a Tanácsnak, az Európai Gazdasági és Szociális Bizottságnak és a Régiók Bizottságának – Európai adatstratégia*. Brüsszel, COM(2020)66 végleges (2020. február 19.).

[156] A 29. cikk szerinti adatvédelmi munkacsoport, Iránymutatás az EUB *Google Spain and Inc kontra Agencia Española de Protección de Datos (AEPD) és Mario Costeja González* C-131/12. sz. ügyben hozott ítéletének végrehajtására vonatkozóan, WP 225, elfogadás időpontja: 2014. november 26. Forrás: az Európai Bizottság honlapja. *Ec.europa.eu.*

Önmagában ugyanis a jogok rögzítését – a kikényszerítés eszközeinek megerősítése, illetve bővítése nélkül – nem tudnánk a védelem erősödéseként, a védelmi lépcsőn való előrelépésként értékelni. Ennek megállapításakor az önkéntes jogkövetés sajnálatos módon meglehetősen alacsony szintjét is figyelembe kell venni.

Az érintetti jogérvényesítést, illetve általában a jogkövetés erősítését szolgáló javaslataimat a továbbiakban részletesen bemutatom.

A központi adatvédelmi nyilvántartások megszűnése, belső nyilvántartások vezetése

A Rendelet új kötelezettségként vezeti be az adatkezelő szervezetek esetében azokat nyilvántartásokat, amelyek az adatkezeléseket áttekintő belső regiszterként értelmezhetők. Nagyban segítik a szervezetek működésének belső áttekinthetőségét, továbbá szerepük van az elszámoltathatóság elvének megvalósításában is. A nyilvántartásokat a Rendelet 30. cikk (4) bekezdése szerint az adatvédelmi felügyeleti hatóság kérése esetén rendelkezésre kell bocsátani.

A belső nyilvántartások bevezetéssel egy időben a Rendelet megszüntette az adatvédelmi hatóságok által korábban vezetett központi nyilvántartásokat. Az előbbi a szervezet belső tudatosságát erősíti, utóbbi pedig erőforrásokat szabadít fel a tagállami hatóságoknál. Mind a két folyamat az erősödő adatvédelmi szint irányába mutat.

A Rendelet (89) preambulumbekezdése szerint a megkülönböztetés nélküli általános jellegű bejelentési kötelezettségeket meg kell szüntetni. Ennek magyarázatát is megadja a jogalkotó ugyanott: „ez a kötelezettség igazgatási és pénzügyi terhekkel jár, azonban nem minden esetben járul hozzá a személyes adatok védelmének javításához".

Álláspontom szerint a felelős adatkezelői magatartás része az adatkezelési műveletek belső nyilvántartásának vezetése. Nem ennek vezetése, hanem kötelező jelleggel való előírása, és ebből fakadó számonkérhetősége jelenti a védelmi lépcsőn való előrelépést.

Az EGT tagállamaiban az adatvédelmi hatóságok többsége elégedetlen a rendelkezésre álló anyagi és humán erőforrásokkal – 30 hatóság közül 21 szerint az erőforrások nem elegendőek, e tekintetben csupán 9 tagál-

lam nyilatkozott elégedetten.[157] Minden olyan szabály, amely ezt a hiányt enyhíti, előrelépésként tartandó számon. A központi nyilvántartások felszámolása önmagában is előrelépés a védelmi lépcsőn, hiszen erőforrásokat szabadít fel.

A központi nyilvántartás tekintetében az irányelvhez képest, amely az ilyen nyilvántartások vezetését és fenntartását elismerte, a rendeleti szabályozás a kedvezőbb fokozatot jeleníti meg a védelmi lépcsőn. Tekintettel arra, hogy a központi nyilvántartás már nem létezik a tagállamokban, a következő szint azonosítása nem lehetséges ezen a téren, azonban rámutat a létező jogintézmények rendszeres felülvizsgálatának szükségességére.

Adatvédelmi hatásvizsgálat

A természetes személyek jogait érintő és valószínűsíthetően magas kockázattal járó adatkezeléseket, különösen, ha új technológiákat alkalmaznak, adatvédelmi hatásvizsgálat *(data protection impact assessment)* alá kell vonni.[158] A hatásvizsgálat elvégzése az adatkezelő feladata. Amennyiben az adatkezelés a kockázatokat mérséklő intézkedések ellenére is magas kockázattal jár, úgy az adatkezelő konzultációt kezdeményez az adatvédelmi hatósággal. A hatóság a konzultációtól függetlenül gyakorolhatja hatásköreit, így többek között megtilthatja az adatkezelést.

Az adatvédelmi hatásvizsgálat növeli a szervezet adatvédelmi tudatosságát. A hatásvizsgálat elszámoltathatósági eszköz: nemcsak a Rendeletnek való megfelelést könnyíti meg, hanem az intézkedések végrehajtásának bizonyítására is szolgál.[159] A kötelező konzultáció kezdeményezése révén a hatóság olyan tervezett adatkezelések esetében is véleményt nyilváníthat, illetve gyakorolhatja hatáskörét, amelyek a hatásvizsgálat intézménye nélkül

[157] Az Európai Adatvédelmi Testület: *Contribution of the EDPB to the evaluation of the GDPR under Article 97* című dokumentumába. Forrás: az Európai Adatvédelmi Testület (EDPB) honlapja.

[158] A kötelezettség részletes szabályait a Rendelet 35. és 36. cikke szabályozza.

[159] Vö. A 29. cikk alapján létrehozott Adatvédelmi Munkacsoport iránymutatása az adatvédelmi hatásvizsgálat elvégzéséhez és annak megállapításához, hogy az adatkezelés az (EU) 2016/679 rendelet alkalmazásában „valószínűsíthetően magas kockázattal jár-e". Az elfogadás időpontja: 2017. április 4. A magyar nyelvű dokumentum forrása a NAIH honlapja.

látókörén kívül maradnának.[160] A hatáskörgyakorlás révén pedig olyan jogsértések előzhetők meg, amelyek valóban kockázatot jelentenek az érintettekre. Mindezek az erősödő védelem irányába mutatnak, és egyértelműen megkülönböztethetők attól a szinttől, ami a Rendelet előtt létezett.

A 95/46/EK adatvédelmi irányelv nem ismerte az adatvédelmi hatásvizsgálat intézményét. Így az irányelv a védelem alacsonyabb, míg a Rendelet a magasabb szintjét valósítja meg a védelmi lépcsőn. A következő szintként az határozható meg, hogy az adatvédelmi hatásvizsgálat – az üzleti titkok tiszteletben tartása mellett – az érintettek számára olyan módon válik megismerhetővé, hogy a várható hatások felmérésének fázisában már előzetesen lehetőségük lesz véleményt nyilvánítani. Ilyen módon nemcsak a szűk értelemben vett jogi megfontolások, hanem az érintett közösség szempontjai is megjelennek az intézkedéseket megelőző mérlegelésekben.[161]

Az adatvédelmi tisztviselő

Az adatvédelmi tisztviselői pozíció nem volt ismeretlen az Európai Unióban a Rendelet előtt sem, több tagállamban már működtek hasonló funkcióban szakértők egyes adatkezelőknél.[162]

A Rendelet bizonyos adatkezelőknél kötelezővé, mások esetében lehetővé teszi a tisztviselő kinevezését. Kötelező a kinevezés közhatalmi és közfeladatot ellátó szerveknél, rendszeres és szisztematikus megfigyelést végző adatkezelőknél, továbbá ott, ahol a személyes adatok különleges kategóriájába tartozó vagy bűnügyi személyes adatot nagy számban kezelnek. A tisztviselő kinevezésére, jogállására és feladataira vonatkozó részletes szabályokat a Rendelet 37–39. cikkei rögzítik. Legfontosabb feladata az adatkezelő támogatása tanácsokkal, továbbá egyfajta belső ellenőri feladat ellátása, amikor saját kezdeményezésre vagy érintetti panasz nyomán a szervezeten belül vizsgálatot folytat. Együttműködik az adatvédelmi hatósággal, inci-

[160] Hasonlóan az adatvédelmi incidensek bejelentési kötelezettségét megelőző időszak incidenseihez.

[161] Összhangban a Rendelet (47) preambulumbekezdésében szereplő „számíthat-e észszerűen" fordulattal.

[162] Magyarországon az Infotv., valamint az egészségügyi és a hozzájuk kapcsolódó személyes adatok kezeléséről és védelméről szóló 1997. évi XLVII. törvény a belső adatvédelmi felelősök kinevezését kötelezővé tette bizonyos esetekben.

dens esetén az érintettek rendelkezésére áll tájékoztatás céljából. Jogállása a szervezeten belül függetlenséget biztosít számára.

A tisztviselő nagyban hozzájárul ahhoz, hogy az adatvédelmi ismeretek házon belül ismertté váljanak, a belső folyamatok kialakítása és döntések meghozatala során adatvédelmi szempontú tanácsait a vezetés rendelkezésére bocsátja. Az érintettekkel és a hatósággal való kapcsolata is hozzájárul ahhoz, hogy az adatkezelő szervezet magasabb szintű adatvédelmet biztosítson működése során. Az adatvédelmi tisztviselő működése a szervezeten belül nagyban növeli annak esélyét, hogy az adatvédelem szintje erősödhessen, így például az egyébként nehezen kikényszeríthető jogok érvényesülhessenek. A közjó megvalósulásának követelménye és az átláthatóság elvárása a jól működő tisztviselői pozíció egyik eredménye lehet az adatkezelő szintjén.

Az adatvédelmi tisztviselői intézmény hiánya, amely az irányelvi időszakban az EGT-tagállamok többségét jellemezte, egyértelműen egy alacsonyabb szintet jelent a védelmi lépcsőn. Az adatvédelmi tisztviselő működése a Rendeletben meghatározottakhoz képest továbbfejleszthető, és véleményem szerint továbbfejlesztendő is, a későbbi fejezetben leírtak minőségi előrelépést valósítanak meg a védelmi lépcsőn, amelyet a következő, kívánatos szintként azonosíthatunk.

A harmadik országba irányuló adattovábbítások szabályainak egységesítése

A Rendelet a harmadik országba[163] irányuló adattovábbítások szabályait egységesíti, egyszersmind a korábbinál részletesebben határozza meg azokat. A szabályozás célul tűzi ki a védelem kiterjesztését az Európai Unión kívüli területekre, mindazonáltal rugalmas lehetőségeket kínál a védelmi szint megteremtésére olyan országokban, ahol egyébként az uniós védelmi szint nem érvényesül. A külföldre irányuló adattovábbítás részletes szabályait a Rendelet 44–49. cikkei rögzítik. A jogalkotó célja az, hogy külföldre irányuló adattovábbítás esetén ne sérüljön a természetes személyek unióban biztosított védelmi szintje, és annak fenn kell maradnia akkor is, ha a harmadik országból egy következő országba továbbítják ismét

[163] A Rendelet a harmadik országokba vagy nemzetközi szervezetek részére történő továbbítást szabályozza, így pontos és teljes a kifejezés jogi értelemben.

az adatokat.[164] Bár a szabályok gyakorlatias jellegüknél fogva inkább életszerű, semmint merev és szigorú eljárásrendet rögzítenek, mégis, az irányultsági szabályokkal kiegészülve az Európai Unióval gazdasági kapcsolatban álló térségekben a magasabb szintű védelem lehetőségét teremtik meg – az adatok szabad áramlásával egyidejűleg.

A megfelelő védelmi szintet biztosító övezet bővítésének kockázata is van, amely a szabadkereskedelmi törekvések és megállapodások, valamint a jogvédelem metszéspontjában fedezhető fel. E kérdések részben már a politikai megfontolások körébe esnek, ezért értelemszerűen nem tárgyai az elemzésnek. E helyütt annak megállapítására szorítkozom, hogy amennyiben például a szabadkereskedelmi célokat szolgáló gazdasági-politikai megfontolások befolyásolhatják a harmadik ország védelmi szintjéről folyó szakértői értékelés kimenetelét, addig nem a jogi, hanem inkább az előbb említett érvek nyomnak többet a latban. Összességében tehát úgy kell tekintenünk az adattovábbítás szabályainak módosulására, mint amely számos más feltétel fennállása esetén járul hozzá az európai uniós és az unión kívül tartózkodó személyek jogvédelmének erősítéséhez, a védelmi szint emeléséhez. E feltételek között említhetjük a gazdasági-politikai nyomás mellett az adatimportőr állam szerveinek együttműködését, tehát azt, hogy a célország jogszabályai és gyakorlata nem üresítik ki a védelem tartalmát. A védelem valós érvényesülésében az adatvédelmi kultúra általános állapota is szerepet játszik.

Az adatvédelmi irányelvvel összehasonlítva a Rendelet nem tekinthető egyértelmű előrelépésnek vagy visszalépésnek a védelmi lépcsőn. A külföldre irányuló adattovábbítás egy olyan komplex terület, amelyre a védelmi lépcső csak egy aprólékos, részletes elemzés alapján lenne alkalmazható. Ehelyütt csak azt állapítom meg, hogy az EU-ban elért védelmi szintet megerősíti a harmadik országba irányuló szabályok helyes és következetes alkalmazása, az adatok exportja ilyen esetben nem jár a védelem eróziójával.

Az EU által elért védelmi szint megőrzése nagyban függ az adatimportőr állam szabályozásától, a piaci szereplők magatartásától. Az Amerikai Egyesült Államok vonatkozásában egyértelmű kudarc, hogy az Európai Unió Bírósága 2020-ban már második alkalommal nyilvánította érvénytelenné az Európai Bizottság határozatát, amelyben az amerikai oldalon

[164] Rendelet (101) preambulumbekezdés.

biztosított védelmi szintet megfelelőnek fogadta el.[165] Ez is megerősíti, hogy ez a téma messze túlmutat egy vázlatosan elvégzett elemzésen.

Független adatvédelmi felügyeleti hatóságok

Az európai uniós rendeleti szabályozás közvetlenül alkalmazandó. A hatóságok feladat- és hatáskörének rendeleti szintű szabályozása jelentős újítás az adatvédelmi jog terén.[166] A hatóságok minden tagállamban azonos feladatokat látnak el és azonos hatásköröket gyakorolnak. A hatáskörök bővülnek a Rendelet következtében, így az adatvédelmi incidens vagy az adatvédelmi hatásvizsgálat, a magatartási kódexek vagy a tanúsítás kapcsán. A figyelmeztetés és az elmarasztalás, a tanúsítvány visszavonása (vagy visszavonatása a tanúsítószervezettel) szintén új hatáskört jelent, ahogyan az általános adatvédelmi kikötések elfogadása és a szerződéses rendelkezések engedélyezése is. Az éves világpiaci forgalom 4%-áig, illetve 20 millió eurós összegig terjedő bírságplafon szerte az unióban erőteljesen kibővítette a hatóságok szankcióit.

Az adatvédelmi felügyeleti hatóságok az intézményrendszer fontos elemét képezik, a hatóságok hatásköreinek bővítése egyértelműen növeli az esélyét a hatékony hatósági fellépésnek, illetve a súlyos szankciók már önmagukban is a jogkövetésre való hajlandóságot erősítik.

A hatóságok feladat- és hatáskörének egységesítése nem hordozza annak kockázatát, hogy az a védelem szintjére adott esetben rossz irányban hatna. Ennek oka, hogy a hatáskörök bővítése minden tagállamban a hatósági mozgástér bővülésével jár, védelmi veszteség vagy kockázat ilyen módon nem jelenik meg.

Meg kell említeni azt a megfontolást is, amely szerint a tagállami jogalkotó az adatvédelmi felügyeleti hatóság hatáskörét a Rendeletben foglaltakhoz képest tovább bővítheti. Ez is garanciája annak, hogy a védelem ezen a téren ne járjon a visszalépés kockázatával.

[165] Data Protection Commissioner versus Facebook Ireland Ltd, Maximillian Schrems, Az Európai Unió Bíróságának ítélete, C-311/18. sz. ügy, ECLI:EU:C:2020:559. Ezt az ítéletet Schrems II döntésként is említik. A Schrems I.-ügyben az EUB az EU és az USA között korábban fennálló, úgynevezett Safe Harbor jogi keret érvénytelenségét állapította meg.

[166] A hatóságok feladatait a Rendelet 57. cikke, a hatóságok hatásköreit az 58. cikke szabályozza.

A védelmi lépcsőn a rendeleti szabályok egyértelműen előrelépést jelentenek, hiszen erősítik a hatóságok szerepét és mozgásterét. Ebben a tekintetben világos előrelépés a Rendeletben foglalt szabályozás az irányelvhez képest. Ezt itt leegyszerűsítve is kijelenthetjük, ugyanakkor később részletesen is kifejtem ennek részleteit, és azt is bemutatom, hogy a hatékonyabban működő, bizonyos hatásköreit megerősített módon gyakorló hatóság a védelem szintjét milyen módon tudná tovább erősíteni.

Adatvédelmi felügyeleti hatóságok együttműködése határon átnyúló adatkezelés esetén

A Rendelet nem csupán a hatóságok feladat- és hatásköreit egységesítette, hanem bizonyos esetekben közös hatáskörgyakorlást ír elő, és ennek eljárási alapjait is megteremti. Az egyablakos ügyintézés[167] során a tevékenységi központ szerinti fő felügyeleti hatóság által készített határozattervezetet a többi érintett hatóság[168] vétójog birtokában véleményezi. A hatóságok egyet nem értése esetén a döntés az Európai Adatvédelmi Testület kezében van, amely kötelező döntést hoz az ügyet érintő vitás jogkérdésekben. A testületi döntésben valamennyi adatvédelmi felügyeleti hatóság részt vesz, azokban többségi álláspont érvényesül. A 96/46/EK számú adatvédelmi irányelvhez képest ez jelentős előrelépés, hiszen lépésről lépésre épül az az esetjog, amely a Rendelet egységes alkalmazását eredményezi. Ilyen módon megvalósul a jogalkotói cél, a harmonizáció a tagállamokban, amely nélkül nem képzelhető el az egységes és magas szintű védelem.[169] Az egységesítés megteremti az egységes védelmi szintet, ami azonban a korábbiakhoz képest – tagállami szinten – a visszalépés kockázatát is hordozza.

Az egyablakos ügyintézés 60. cikk szerinti eljárásán túl a hatóságok az úgynevezett kölcsönös segítségnyújtási eljárás és a közös műveletek révén

[167] Az eljárásrendet a Rendelet 60. cikke szabályozza. Az eljárás arra irányul, hogy a fő felügyeleti hatóság és az érintett hatóságok együttműködésében egyetlen döntés szülessen, amelynek hatálya aztán az egész Európai Gazdasági Térségre kiterjed, ilyen módon is biztosítva a Rendelet egységes alkalmazását.

[168] Érintett az a hatóság, ahol a vizsgált adatkezelőnek van tevékenységi helye, ahol az adatkezelés jelentős mértékben érint adatalanyokat (vagy ez valószínűsíthető), illetve panaszt nyújtottak be az adott ügyben a felügyeleti hatósághoz (Rendelet 4. cikk 22. pont).

[169] Az Európai Adatvédelmi Testület hatáskörét a Rendelet 70. cikke, eljárásait pedig a 64. és 65. cikk szabályozza.

hatékonyan tudják felhasználni a többi hatóságnál rendelkezésre álló tudást és erőforrást.[170] A hatósági működés egyik problémája a hatékonyság. Nagyban hozzájárul a hatékonyabb működéshez az együttműködési eljárások új rendje. Az együttműködés önmagában is lehetőséget ad a szinergiák kihasználására, a párhuzamosságok megszüntetésére és a közös tudás hatékony használatára.

A hatékonyabban működő hatóságok, ahogyan utaltunk már rá, jelentős mértékben képesek erősíteni a személyes adatok védelmét. Az egységes joggyakorlat pedig jótékonyan hat a jogbiztonságra, amely a jogkövetést erősíti. Az egyablakos ügyintézés a 95/46/EK irányelv idején tömegesen előforduló párhuzamos eljárások problémáját küszöböli ki. Egy adott jogkérdésben csupán egy és egységes jogi álláspontot alakítanak ki az eljáró hatóságok. Ez mindenképpen védelmi többlettel jár, még akkor is, ha a hatósági döntéssel szemben az érintett számára elérhető jogorvoslat lehetősége megnehezül.

Amennyiben egy magyar érintett határon átnyúló adatkezelést kifogásoló panasza nyomán induló eljárásban az osztrák adatvédelmi felügyeleti hatóság hoz határozatot, akkor az ellen az adatalany az osztrák közigazgatási eljárás szabályai szerint az osztrák közigazgatási bíróság előtt terjeszthet elő jogorvoslati kérelmet. Ez az érintetti joggyakorlást jelentősen megnehezíti ezekben az esetekben.

Az EGT-tagállamok adatvédelmi hatóságainak együttműködése tehát az az egyik *differentia specifica,* amely révén a védelmi szintek közötti különbség tetten érhető, és a védelmi lépcsőn való előrelépésként azonosítható.

Az adatvédelmi incidensek bejelentésének kötelezettsége

Az adatvédelmi irányelv nem ismerte az incidensek bejelentésének általános kötelezettségét. Egyes országokban, illetve ágazatokban már létezett ilyen bejelentési kötelezettség, azonban általános jelleggel még nem kellett az adatvédelmi incidenseket az adatvédelmi felügyeleti hatóságok tudomására hozni. Ebben az esetben is egy szabályozási hiányossággal szembesültünk, amelyet a 2015-ös közvélemény-kutatás is alátámasztott.

[170] A kölcsönös segítségnyújtási eljárás szabályait a Rendelet 61. cikke, a közös műveleteket a 62. cikke szabályozza.

A megkérdezettek 91%-a (2010-ben is már 87%-a) volt azon a véleményen, hogy szeretne tájékoztatást kapni arról, ha adatait elvesztik vagy ellopják.[171]

Az elektronikus hírközlési szektorban az Európai Parlament és a Tanács 2002/58/EK irányelve (2002. július 12.), az elektronikus hírközlési ágazatban pedig a személyes adatok kezeléséről, feldolgozásáról és a magánélet védelméről szóló elektronikus hírközlési adatvédelmi irányelv 2013-as módosítása teremtette meg Európai Unió-szerte a bejelentési kötelezettséget. A Rendeletet megelőzően általános adatvédelmiincidens-bejelentési kötelezettség az Egyesült Királyságban, Németországban és Hollandiában volt életben, Írországban gyakorlatilag önkéntes alapon működött a bejelentés rendszere.[172]

A védelmi lépcsőn az ágazati szabályozást tekinthetjük egy fontos, előhírnök szabályozási fokozatnak,[173] amelynek továbbfejlesztése az általános bejelentési kötelezettség. Ez több tekintetben is előrelépést jelent, és megkülönböztethető az első fokozattól (ebben az esetben azonosítható az ágazati szabályozásokat is megelőző időszak szabályozása is mint még korábbi fokozat). A bejelentési kötelezettség azt eredményezi, hogy az adatkezelő szervezetek belső eljárásrendjükben rögzítik a bejelentés menetét az incidens észlelésétől kezdve. Önmagában az, hogy egy külső szereplő felé is elszámoltatható az adatkezelő, növeli a tudatosság szintjét. Az érintettek bevonásának kötelezettsége szintén a tudatosság és a transzparens működés irányába mutat. A hatóság számára a bejelentések egy új, az eddigieknél tárgyilagosabb forrást jelentenek a napi adatkezelési műveletek világából.

[171] Special Eurobarometer Report (431): Data Protection (Adatvédelem). *Europa.eu/eurobarometer,* 2015. 72–73.

[172] Árvay Viktor et al.: *Az új általános európai adatvédelmi szabályozás és az adatkezelői kötelezettségek*. Budapest, NKE, 2018. 79., illetve a holland bejelentési kötelezettségről bővebben, forrás: a holland adatvédelmi hatóság honlapján elhelyezett tájékoztató.

[173] A 2002/58/EK irányelv szabályait elemezte a 29. cikk szerinti munkacsoport 3/2014-es számú véleményében. E véleményben hangsúlyozza az incidensek bekövetkezésének megelőzését, a megelőző intézkedések fontosságát és az érintettek tájékoztatásának kötelező eseteit, kockázatalapú megközelítést alkalmazva. A dokumentum még a Rendelet előtt került nyilvánosságra, és jelzi, hogy a hatósági joggyakorlat már kellő felkészültséggel várta az új jogintézmény bevezetését. Forrás: az Európai Bizottság honlapja.

Az adatvédelmi felügyeleti hatóságok kötelesek kivizsgálni a panaszokat. Az érkező beadványok jelentős része ebből a forrásból származik. A másik tipikus forrás az adatkezelőké, akik konzultációt, iránymutatást kezdeményező kérelmeket nyújtanak be, amelyekben jogértelmezési kérdésekben kérik a hatóságok iránymutatását. Mind a két forrás valamennyire szubjektív, az incidensek azonban egy olyan eseménysort mutatnak be, amelyek mind az érintettek, mind az adatkezelők szándékától függetlenül valósultak meg.

Az incidensekben feltárt tényeket a hatóságok elemzik, és a kockázatok mértékétől függően kötelezhetik az adatkezelőt az érintettek tájékoztatására. Az incidensek révén arra is lehetőség nyílik, hogy az adatkezelést közelebbről is megvizsgálja a hatóság, adott esetben hivatalból is kiterjessze vizsgálatát olyan körülményekre, amelyek az incidens révén kerültek látókörébe. Egyébként is, a hatóságok az incidensek bejelentése révén olyan jogsértésekkel találkoznak, amelyek korábban, a védelmi lépcső alacsonyabb szintjén nem jutottak el a hatóságokhoz.

Az említett szinteken túl nem tudok javaslatot megfogalmazni a következő védelmi szintre vonatkozóan. Ennek oka, hogy a bejelentési kötelezettség eddigi gyakorlata nem szolgált olyan tapasztalattal, amelynek alapján az új szint a rendeleti szabályozáshoz képest meghatározható lenne.

Adatvédelmi bírság

A Rendelet szankcióinak hatékonynak, arányosnak és visszatartó erejűnek kell lenniük.[174] Ezt a célt szolgálja a bevezetett, korábban egyik tagállamban sem ismert mértékű adatvédelmi bírság. Enyhébb esetben 10 millió euró, vagy az előző év világpiaci forgalmának 2%-a, súlyosabb esetben 20 millió euró, illetve a világpiaci forgalom 4%-a a bírságplafon. A Rendelet kifejezetten ösztönzi a tagállami adatvédelmi hatóságokat arra, hogy tudatosan éljenek a szankciók alkalmazásával. Annak alkalmazása azonban nem lehet rutinszerű, hiszen a túlzottan gyakori bírságok a jogintézmény funkciójának

[174] A Rendelet 83. cikk (1) bekezdése, valamint a 84. cikk (1) bekezdése is előírja ezt a követelményt.

erodálódásával járhatnak.[175] A visszatartó erejű szankciók egyértelműen az erősebb védelem irányába mutatnak.

A hatóságoknak a szankciók terén kibővített mozgástere önmagában is a védelem erősödésével jár az irányelvi szabályozáshoz képest, és a bírságok maximális mértéke a védelmi lépcső elmélete alkalmazásakor a legegyszerűbben mérhető indikátorként jelenik meg. Azt is hozzá kell tennünk, hogy az irányelvi szabályozás idején a tagállamok közötti gyakorlat változó volt, közel sem volt egységes. Az egységesítés önmagában is a kedvezőbb jogérvényesítés lehetőségét kínálja. A következő védelmi szint meghatározására a későbbi fejezetekben kitérek.

Az adatvédelmi szabályozás technológiai fejlődést és változó üzleti modelleket követő rendszeres felülvizsgálata

A személyes adatok védelmét szolgáló szabályok természetszerűleg egy változó közegben valósulnak meg. A privacy védelme a technológia és az alkalmazott üzleti modellek hatásainak egyik leginkább kitett jogterület. Ez már a jog születésekor megmutatkozott, és végigkíséri a jog alakulását.

Az előbbiek alapján a mindenkori adatvédelmi szabályozással szembeni alapvető elvárás, hogy időszakosan felülvizsgálja és az aktuális technológia fényében értékelje a szabályozás alkalmazását a jogalkotó. Mind az adatvédelmi irányelv, mind pedig a Rendelet tartalmaz ilyen szabályokat.

> Az adatvédelmi irányelv úgy rendelkezett, hogy a „Bizottság rendszeresen, és első alkalommal legkésőbb a 32. cikk (1) bekezdésében említett időponttól számított három évvel jelentést tesz a Tanácsnak és az Európai Parlamentnek az irányelv végrehajtásáról, jelentéséhez szükség esetén csatolva a módosításokra irányuló megfelelő javaslatokat. A jelentést nyilvánosságra kell hozni. A Bizottság megvizsgálja ezen irányelvnek különösen a természetes személyekkel kapcsolatos hang- és képadatok adatfeldolgozására történő alkalmazását, és benyújtja az informatika terén elért fejlesztéseket figyelembe véve az infor-

[175] A közigazgatási bírság alkalmazásáról és megállapításáról szóló 29-es munkacsoporti iránymutatás (WP 253, elfogadás időpontja: 2017. október 3.) úgy fogalmaz, hogy a hatóságok a bírságot ne használják „olyan módon, amellyel lerontják eszközként való használatuk hatékonyságát" (7.). Forrás: a NAIH honlapja.

mációs társadalom elért fejlődési szintjére tekintettel szükségesnek bizonyuló megfelelő javaslatokat."

A két jogszabály szövegét összehasonlítva azt látjuk, hogy bár a Rendelet részletesebb szabályokat tartalmaz, lényegében a jogalkotó hasonló célból kötelezi az Európai Bizottságot jelentés elkészítésére.

Az irányelvi szabályokkal összehasonlítva többletként jelenik meg, hogy a Bizottság a felülvizsgálat során információkat kérhet a tagállamoktól és a felügyeleti hatóságoktól. A Bizottság az értékelések és felülvizsgálatok során figyelembe veszi az Európai Parlament, a Tanács és az egyéb érintett szervek vagy források álláspontját és megállapításait. A Bizottság a módosításra irányuló javaslatok megfogalmazása során figyelembe veszi az információs technológia fejlődését és az információs társadalom fejlődési szintjét.

Álláspontom szerint e szabály nélkülözhetetlen eleme a magas szintű védelemnek. Az is látható azonban, hogy az adatvédelmi irányelvet nem módosították 1995 és 2011 között. Az irányelv alkalmazását követő bő másfél évtized után egy teljesen új szabályozás kialakításába kezdett az uniós jogalkotó, és így született meg az itt is tárgyalt Rendelet. Az előkészítő munkálatok és a Rendelet alkalmazandóvá válása között mintegy nyolc év telt el. A jogalkotó uniós szinten a háromévente elkészített egyik jelentés nyomán sem módosította az irányelvet. Kérdés, vajon a Rendelet négyévente esedékes értékelése és felülvizsgálata vezet-e majd érdemi felülvizsgálathoz és a jogalkotási aktus módosításához.

Nem azt állítom, hogy a jogi normák szövegét gyakran módosítani szükséges. Azt azonban követelményként fogalmazhatjuk meg a szabályozás minőségével kapcsolatban, hogy érdemi, a lehetséges módosítás esélyét is magában foglaló felülvizsgálatra van szükség ahhoz, hogy a szabályozás korszerűnek legyen mondható, amely a védelem szintjét változó körülmények között is szavatolja. Az irányelvet kísérő másfél évtizedes jogalkotói „hallgatást" követően némi gyanakvással figyelhetjük, hogy a Rendelet szabályait milyen eredménnyel fogja felülvizsgálni a jogalkotó.

Ami a védelmi lépcső alkalmazását illeti, a jelenlegi elemzés és tapasztalat arra vezet, hogy az irányelv nem felelt meg annak az elvárásnak, amelyet leírtam. Ehhez képest a Rendelet lényegét tekintve megismétli a korábbi szabályozást. Amennyiben a gyakorlat igazolja majd a Rendeletet övező várakozásokat, és érdemi felülvizsgálatra kerül sor, úgy a Rendelet

e tekintetben a védelmi lépcsőn előrelépést jelent majd. Ezt azonban egyelőre nem tudjuk kijelenteni, ezért elemzésem arra vezetett, hogy jelenleg az egy helyben toporgás jellemzi az uniós jogalkotó eljárását. Ez annál is inkább sürgetően orvosolandó mulasztás, mert a szabályozás megmerevedése – a változó technológiai és piaci környezetben – szükségszerűen vezet a védelem eróziójához. Ilyen módon nem valósul meg az a jogalkotói célkitűzés, hogy a védelem magas szintjét biztosítsa a tagállamokban. Azt kell megállapítani, hogy a technológiai és az információs társadalomban végbemenő változásokra való reagálás képtelensége önmagában is csökkenő védelmi szintet eredményez.

Összegzés

Az előzőekben áttekintettem a Rendelet egyes szabályait és jogintézményeit. A Rendelet a védelmi szint erősítésének szándékával született, azonban látható, hogy több ponton maga az új szabályozás is különböző kockázatokat hordoz a védelmi szint tekintetében. Ezeknek a kockázatoknak a mérséklése és kiküszöbölése nagyban múlik azon, hogy az egyes szereplők, így az adatkezelők és adatfeldolgozók, az adatvédelmi tisztviselők, a felügyeleti hatóságok, vagy éppen a jogalkotó milyen mértékben élnek a Rendelet adta lehetőségekkel, mennyiben érvényesítik annak szabályait.

A harmonizációra való törekvésnek vannak ugyan kockázatai, mégis, az egységes szabályozás és gyakorlat nagyban a tagállami jogalkotón, illetve jogalkalmazón is múlik. A Rendelet eredeti, az Európai Bizottság tervezetében megjelenő koncepciója szerint nagyon kevés eltérést engedett volna tagállami szinten. A jogalkotási folyamat során ez a kötöttség oldódott a hatáskörök egy részének tagállami szinten tartása révén. Ha ezek a hatáskörök tagállami szinten mégsem vezetnek erős harmonizációhoz, akkor a szétaprózódott és inkoherens jogalkotás révén az a helyzet állhat elő, amelynek orvoslása a Rendelet eredeti célkitűzése volt.[176]

A Rendelet megteremti a magas védelmi szint lehetőségét, azonban a felépített rendszer sérülékeny. Az elkövetkező évek gyakorlata alapján lehet majd megítélni, hogy a Rendelet összességében a magánszféra védelmének erősítésével járt-e. Ez egyelőre bizonytalan még, ezért nem is vonok le további következtetéseket.

[176] A Rendelet (9) preambulumbekezdése írja le ezt a jelenséget, illetve kritikát.

A következő fejezetekben részletesen elemzem az adatvédelmi tisztviselő és az adatvédelmi hatóságok új szabályozását, ez utóbbi témakörben kitérve az adatvédelmi bírság új szabályaira is. Elemezni fogom, hogy ezek az intézmények milyen szerepet töltenek be a védelem rendszerében, miként járulnak hozzá a jogok érvényesítéséhez, és miképpen erősítik – ha erősítik – a védelem szintjét. Mindezt az elemzést a védelmi lépcső elméletének fényében végzem el. Elemzésemnek az a célja, hogy olyan új védelmi szintet azonosíthassunk, ami jogilag megvalósítható, és a jelenlegi szabályozásnál hatékonyabban szolgálja a magánszféra védelmét.

Vákát

A Rendelet egyes jogintézményeinek részletes elemzése – az adatvédelmi tisztviselő

Az a gyanakvás, hogy az adatkezelő szervezetek átláthatóságát illetően deficit mutatkozik, évtizedekre nyúlik vissza. 1965-ben Harold D. Lasswell fogalmazta meg, hogy „az információk nyilvánosságra hozatala arról, hogy hogyan manipulálják a manipuláltakat, messze túlmutat a politikai arénán".[177] A belső információkhoz való hozzáférés és a döntéshozatal figyelemmel kísérése nem a 21. század sajátos követelése.

A tisztviselői intézmény egyértelműen a védelem erősítésének szándékával jött létre. Peter Hustinx a tisztviselőket olyan szereplőként mutatja be, akik az „első vonalban" végzik munkájukat, és az ő hálózatuk nagyon hasznos tapasztalattal szolgál más szereplők, így az adatvédelmi hatóságok számára is.[178]

Daniel Le Métayer a magánszférát érintő problémák elemzésekor négy szereplőt különböztet meg egymástól: az egyének, a jogászok, az informatikai szakértők és az ipari szereplők csoportját, vagy másként fogalmazva: a társadalom, a jog, a technológia és a piac.[179] Ez az áttekintés hasznos kiindulópontja a magánszféráról való értekezéseknek, és bár Le Métayer a *privacy by design* kontextusában értekezett erről, a tisztviselők kapcsán is hasznát tudjuk venni. A tisztviselő ugyanis az a szereplő, aki mind a négy csoporthoz közel áll. Szerepéből adódóan könnyen megismerheti e négy csoport igényeit, és ő van abban a helyzetben, hogy ebből az érdekegyüttesből optimális megoldási javaslatot tudjon megfogalmazni.

[177] Harold D. Lasswell: Policy Problems of a Data-Rich Civilization. In Alan F. Westin (szerk.): *Information Technology in a Democracy*. Cambridge, Massachusetts, Harvard University Press, 1971. 191.

[178] Peter Hustinx: The Role of Data Protection Authorities. In Serge Gutwirth et al. (szerk.): *Reinventing Data Protection*? Amsterdam, Springer, 2009. 135.

[179] Daniel Le Métayer: Privacy by Design: A Matter of Choice. In Serge Gutwirth – Yves Poullet – Paul De Hert (szerk.): *Data Protection in a Profiled World*. Amsterdam, Springer, 2010. 328–329.

Az adatvédelmi tisztviselői intézmény

A Rendelet 2018. május 25-étől alkalmazandó szabályai szerint az adatvédelmi tisztviselő kinevezése számos adatkezelő esetében kötelezővé vált. Az International Assosiation of Privacy Professionals (IAPP) előzetes kalkulációja szerint a Rendelet alkalmazása érdekében az adatkezelő szervezetek, beleértve a közhatalmi szerveket is, világszerte 75 ezer adatvédelmi tisztviselőt kell hogy alkalmazzanak.[180] Az Európai Unió intézményeiben kötelesek adatvédelmi tisztviselőt kinevezni, ez a kötelezettség már csaknem két évtizede létezik.[181]

Az adatvédelmi tisztviselő jelenléte és munkássága az adatvédelmi kultúra szerves része. Az adatkezelő szervezetek kívülről szemlélve csak egyfajta „fekete doboz" jelleggel működnek sok esetben, nem követhető, hogy az egyén adatait milyen módon kezelik, értékelik és használják fel. Ilyen körülmények között szükség van arra, hogy valaki belelásson e folyamatokba, és szakértő módon mozdítsa elő a tisztességes és törvényes adatkezelés ügyét.

A *black box* jelenség különösen a mesterséges intelligencia (MI, Artificial Intelligence – AI) területén vet fel újabban aggályokat. Az átláthatatlanság, az összetettség, a kiszámíthatatlanság és a részben autonóm viselkedés az MI sajátja. Az Európai Bizottság az MI és minden más területen azon dolgozik, hogy a gyártók, felhasználók számára jogbiztonságot, a fogyasztók, érintettek számára pedig olyan környezetet teremtsen, ahol az új technológiákat magukban foglaló termékeket, szolgáltatásokat bizalommal vásárolhatják meg.[182]

Az alábbiakban bemutatom, hogy a tisztviselő miképpen képes hozzájárulni a szervezeten belül az adatkezelések jogszerűségének biztosításához, valamint az érintetti jogok gyakorlásához. A védelmi lépcső elméletének figyelembevételével mindenképpen előrelépésnek tekintendő, ha egy adott országban az intézmény meghonosodik.

[180] The GDPR demands 75k DPOs – Where Will They Come From? *Iapp.org.*

[181] Az Európai Parlament és a Tanács EK/45/2001. számú rendelet 24. cikke rendelkezett arról, hogy minden uniós intézmény és uniós szerv köteles adatvédelmi tisztviselőt kinevezni.

[182] Vö. Az Európai Bizottság fehér könyve: *On Artificial Intelligence – A European approach to excellence and trust.* Brüsszel, COM(2020)65 végleges, 12. (2020. február 19.)

Elemzésemben az elérhető szakirodalom és joggyakorlat mellett alapvetően a Rendelet normaszövegére, a vonatkozó preambulumbekezdésekre mint értelmező rendelkezésekre támaszkodok, továbbá az egyes értelmezési kérdésekben hivatkozok az Európai Adatvédelmi Testület adatvédelmi tisztviselőről szóló iránymutatására.[183]

Kockázatok és elszámoltathatóság

A Rendelet kapcsán gyakran említjük a kockázatalapú megközelítést mint jogalkotói koncepciót, valamint az elszámoltathatóság elvét, amely átszövi a Rendelet valamennyi rendelkezését.

A kockázatokról, amint arról fentebb szóltam, a Rendelet preambulumbekezdéseiben találunk egy részletes felsorolást. A jogalkotó a privacyt fenyegető kockázatokat veszi számba, amelyek a Rendelet tekintetében mindvégig egyfajta zsinórmértékül szolgálnak: addig, amíg a személyes adatok kezelése kapcsán ezek a jelenségek előfordulhatnak, a védelem indokolt, és végső soron ez adja az adatvédelmi intézkedések legitimitását.

Az adatkezelő tevékenységének értékelése során az elszámoltathatóság elve is érvényesítendő. Az elszámoltathatóság lényege abban ragadható meg, hogy a jogalkotó szándéka szerint az adatkezelés végrehajtása során egyrészt érvényesül a Rendelet szabályrendszere, másrészt pedig a szervezet képes arra, hogy ezt világosan és egyértelműen bemutassa. Az érintett helyzete és várakozásai fontosak a megfelelés szempontjából, ez a Rendelet (47) preambulumbekezdésében is érvényre jut, amikor a jogalkotó a „számíthat-e észszerűen" fordulatot használja. Ez mércéje is az adatkezelés jogszerűségének, mert ha erre megnyugtató válasz adható az adatalanynak, úgy az adatkezelés feltehetően nem jogellenes, illetve elejét lehet venni az érintetti panaszoknak, amelyek tipikus esetben kiindulópontjai jogvitáknak, illetve a hatósági eljárásoknak. A tisztviselő jelenléte és munkássága az érintettek körében végzett kutatás szerint hozzájárulhatna az adatok védelmének erősítéséhez. A megkérdezettek 64%-a válaszolt igennel arra a kérdésre,

[183] A 29. cikk szerinti adatvédelmi munkacsoport: *Iránymutatás az adatvédelmi tisztviselőkkel kapcsolatban, WP 243 rev.01,* az elfogadás időpontja: 2017. április 5. A dokumentumot az Európai Adatvédelmi Testület első, 2018. május 25-i ülésén számos más dokumentummal együtt ünnepélyesen megerősítette. Forrás: az Európai Bizottság (a 29. cikk szerinti munkacsoport titkárságának) honlapja.

hogy véleménye szerint az adatait jobban védenék a nagyvállalatok, ha arra kötelezné őket, hogy egy kijelölt kapcsolattartót nevezzenek ki az adatok megfelelő kezelésének ellenőrzésére.[184]

Az elszámoltathatóság hangsúlyozásával az adatkezelő és adatfeldolgozó oldalán érvényesülő felelősség még világosabban kirajzolódik. Az adatvédelmi tisztviselő olyan belső ellenőrzési mechanizmus letéteményese, amelyre eddig nem volt példa. Ha egy mondatban szeretnénk összefoglalni a tisztviselő szerepét, akkor azt mondhatjuk, hogy az adatvédelmi tisztviselő megkönnyíti a Rendelet rendelkezéseinek való megfelelést.[185] Mindezt a kockázatokra tekintettel, az elszámoltathatóság jegyében teszi.

Az érintettek régi és megerősített, valamint a Rendeletben meghatározott új jogaikkal[186] a korábbiakhoz hasonlóan élhetnek, azonban az elsődleges jogorvoslati lehetőségek egyértelműen az adatkezelő felé tevődtek át. Megnőtt a jelentősége annak, hogy első körben milyen módon lehet megnyugtató megoldást találni az adatkezelő oldalán. Ebben az adatvédelmi tisztviselőnek jelentős szerep jut.

Az adatvédelmi tisztviselők szerepe[187]

Az adatvédelmi Rendelet kiemelt figyelmet fordít azokra az adatkezelő szervezetén belül alkalmazott tisztviselőkre, akik már a Rendelet előtt is nagymértékben hozzájárultak az adatvédelmi szabályok érvényesítéséhez.

A Testület azt állítja, hogy az elszámoltathatóság egyik alapköve a tisztviselői intézmény,[188] és a tisztviselők foglalkoztatása versenyelőnyt jelenthet

[184] Special Eurobarometer Report (359): Attitudes on Data Protection and Electronic Identity in the European Union (Az adatvédelemmel és az elektronikus személyazonossággal kapcsolatos hozzáállás az Európai Unióban). *Europa.eu/eurobarometer,* 2011. 186–189.

[185] Testületi iránymutatás az adatvédelmi tisztviselőkkel kapcsolatban, 5.

[186] A Rendelet az adatvédelmi irányelvben felsorolt katalógushoz képest bővíti az érintetti jogokat. Új jogként határozták meg az elfeledtetéshez való jogot *(a right to be forgotten)* az internetes közegben (17. cikk), az adathordozhatósághoz való jog *(right to data portability),* a Rendelet 20. cikkében.

[187] Kapcsolódó jogi szabályozás: a Rendelet 37–39. cikke, továbbá a (97) preambulumbekezdés.

[188] A Rendelet (77) preambulumbekezdése szerint „a megfelelő intézkedéseknek az adatkezelő általi végrehajtásához, valamint a megfelelés általuk való bizonyításához – különösen ami a kockázat beazonosítását, valamint a kockázat súlyosságának a felmérését illeti –, továbbá a kockázat mérséklésével kapcsolatos útmutatással szolgálhatnak különösen a jóváhagyott

az üzleti szereplők számára, továbbá a jelenlétük hasznos a szervezet vezetői számára is. A 29-es munkacsoport tisztviselőkről készített véleményének melléklete kérdések és válaszok formájában foglalja össze a legfontosabb tudnivalókat az adatvédelmi tisztviselőkről. Ez nemcsak a tisztviselőknek lehet hasznos, hanem a szervezeten belüli egyeztetések során is szerepet játszhat, hiszen viszonylag rövid terjedelemben mutatja be a tisztviselővel kapcsolatos legfontosabb tudnivalókat és elvárásokat.

A versenyelőny csak közvetetten fejt ki hatást az adatok védelmére. A jogalkotó célja és reménye, hogy a fogyasztók, akik végső soron az adatalanyok az egyes szolgáltatások kapcsán, az egyéb piaci megfontolások mellett privacy szempontokat is figyelembe vesznek a szolgáltatások kiválasztásánál. Amennyiben az adatkezelő szervezet ebben a minőségében is jól helytáll a versenyben, az remélhetőleg piaci lehetőségeinek bővülésével is jár. Ennek megteremtésében pedig az adatvédelmi tisztviselőnek kiemelt szerep jut.

A tisztviselők maguk személyesen nem felelősek a jogszabályoknak való megfelelésért, az adatkezelőre vagy az adatfeldolgozóra hárul a felelősség az esetleges jogsértésekért.[189] E szabálynak munkajogi vonatkozásai is vannak. Az adatvédelmi tisztviselők szerepe e tekintetben gyakorlati nehézségekhez vezet, ami szintén indokolja e kérdések tisztázását.[190]

A nemzetközi példák azt mutatják, hogy voltak országok, ahol a belső adatvédelmi felelősök intézménye 2016-ot megelőzően még nem honosodott meg, ezért a Rendeletre való felkészülés a tisztviselők képzését is magában foglalta.[191] A Rendeletet megelőzően az EU tagállamai színes képet mutattak ezen a téren. Magyarország már viszonylag korán belépett azon országok sorába, ahol a tisztviselőket (akkori terminológia szerint

magatartási kódexek, a jóváhagyott tanúsítási eljárások, a Testület iránymutatásai vagy az adatvédelmi tisztviselő által nyújtott iránymutatások".

189 Lásd testületi iránymutatás az adatvédelmi tisztviselővel kapcsolatban, 5.

190 Vö. Szabó Endre Győző: Az adatvédelmi tisztviselőről – a GDPR szabályainak elemzése. *Infokommunikáció és Jog,* 70. (2018), 1. 3–10.

191 Az IAPP (International Association of Privacy Professionals) 2016. július 19-én nyilvánosságra hozott elemzése (GDPR conundrums: The Data Protection Officer Requirement) csupán négy európai uniós országot emel ki, ahol kötelező kinevezés érvényesült: Németország, Horvátország, Magyarország és Spanyolország. Még ha az elemzés némiképp vázlatos is, jól mutatja, hogy a tisztviselői pozíció korántsem vált a mindennapi gyakorlat részévé valamennyi tagállamban. Forrás: a Tilburg University honlapja.

belső adatvédelmi felelősöket) ki kellett nevezni. Az adatvédelem terén megszülető publikációk „első generációjában" már megjelent az igény egy olyan, házon belül foglalkoztatott szakértő személyre, adatvédelmi felelősre, akinek „feladata, többek között, a szükséges biztonsági intézkedések kezdeményezése, a titokvédelmi munka felügyelete, és a védelmi előírások megtartásának ellenőrzése". [192]

Magyarországon a személyes adatok védelméről és a közérdekű adatok nyilvánosságáról szóló 1992. évi LXIII. törvény (Avtv.) már 2003 óta előírta bizonyos esetekben a belső adatvédelmi felelős kinevezését, így például országos hatósági adatkezelőnél, pénzügyi szervezetnél, távközlési és közüzemi szolgáltatónál. Az Avtv.-hez hasonlóan az egészségügyi és a hozzájuk kapcsolódó személyes adatok kezeléséről és védelméről szóló 1997. évi XLVII. törvény is előírta az adatvédelmi felelős foglalkoztatását a meghatározott létszámot meghaladó foglalkoztatottal rendelkező szervezeteknél. A Rendeletet megelőzően a 95/46/EK adatvédelmi irányelv nem tette kötelezővé a tisztviselő kinevezését. Ennek megfelelően voltak tagállamok, ahol az adatvédelmi tisztviselői intézmény ismeretlen volt. [193]

Előrelépés a védelmi lépcsőn és az adatvédelmi tisztviselői intézmény léte

Az adatvédelmi tisztviselői intézmény elemzésének első megállapítása részemről, hogy az intézmény meghonosodása önmagában is előrelépésnek tekintendő. A tisztviselői intézmény értékelése a védelmi lépcső elméletének fényében meglehetősen egyszerűnek mutatkozik. Az adatvédelmi irányelv korábban nem tette kötelezővé a tisztviselői intézmény tagállami szinten való létrehozását. Bár utalt arra, hogy például az adatkezelések központi nyilvántartásba vételi kötelezettsége alól mentesítést jelenthet a tisztviselő kinevezése, ez az utalás nem értékelhető még csak a tagállami jogalkotó biztatásaként sem az intézmény megalkotására.

[192] Gömbös Ervin: A számítástechnikai rendszerek titok-, vagyon- és tűzvédelme. *Számítástechnika,* 1981. március.
[193] Vö. Péterfalvi (2012): i. m. 173–176.

Az adatvédelmi irányelv 18. cikk (2) bekezdésében előírta, hogy „[a] tagállamok kizárólag a következő esetekben és feltételek mellett rendelkezhetnek az értesítés módjának egyszerűsítéséről vagy az értesítési kötelezettség alóli felmentésről: […] amennyiben az adatkezelő a rá vonatkozó nemzeti jogszabályokkal összhangban kijelöl egy személyesadat-védelmi tisztviselőt, aki elsősorban az alábbiakért felelős: az ezen irányelv alapján elfogadott nemzeti rendelkezések belső alkalmazásának független módon való biztosítása, az adatkezelő által végzett adatfeldolgozási műveletek nyilvántartásának vezetése, amely tartalmazza a 21. cikk (2) bekezdésében említett adatokat".

Ennek megfelelően a tisztviselői intézményt uniós szinten nem létezőnek, vagy legalábbis csak elvétve és sporadikusan előforduló előírásnak tekinthetjük. Az ilyen uniós szabályozást a védelmi lépcső terén egy alacsonyabb fokozatként kell hogy számontartsuk. Ehhez képest az intézmény kötelező előírása világos előrelépés, a védelmi lépcső második azonosított fokozata. Az intézmény megjelenése a jogi szabályozásban az általunk ismert legmagasabb fok is egyben, ugyanis a létezése időben statikus védelmi komponensként azonosítható.

Mi indokolja, hogy a tisztviselő létét előrelépésnek tekintjük a védelmi lépcsőn? Mindenekelőtt a szervezeten belüli megfelelés támogatása révén megteremti, megerősíti az érintetti joggyakorlás lehetőségeit. Ezen túl az adatvédelmi felügyeleti hatóság munkáját is támogatni tudja, például egy konkrét vizsgálattal, vagy éppen kutatásban való részvétel útján. Mindemellett hangsúlyozni kell a tisztviselői intézmény és a tisztviselői hálózat szerepét az adatvédelmi kultúra megteremtésében. Ezt a szerepet a testület is kiemeli iránymutatásában: „Az adatvédelmi tisztviselő kulcsszerepet játszik a szervezeten belül az adatvédelmi kultúra előmozdításában […]."[194] Az adatkezelő szervezeten belül a tisztviselő munkássága ezen a téren számos lehetőséget rejt. A 29. cikk szerinti adatvédelmi munkacsoport már 2010-ben figyelmeztetett, hogy amennyiben az adatvédelem nem válik az adatkezelő szervezet hétköznapjainak részévé, akkor „az elvek és kötelezettségek hatékony betartása jelentős kockázatnak lesz kitéve".[195] Ennek

[194] Testületi iránymutatás az adatvédelmi tisztviselővel kapcsolatban, 14.

[195] A 29. cikk szerinti munkacsoport 3/2010 számú véleménye az elszámoltathatóság elvéről, elfogadás időpontja: 2010. július 13. 2 és 6. Forrás: az Európai Bizottság (a 29. cikk szerinti munkacsoport titkárságának) honlapja.

biztosítására, az elszámoltathatóság megteremtésére a munkacsoport többek között a tisztviselő kinevezését javasolta.

Hozzá kell tenni, hogy a tisztviselők hálózata a tapasztalatcsere és tanácskozások révén is hozzájárulhat az adatvédelmi szabályok tudatos alkalmazásához. Az adatvédelmi tisztviselők vagy adatvédelmi szakértők hálózatai fontos szakmai fórumot jelentenek. Magyarországon az Infotv. szerint az adatvédelmi hatóság évente legalább egyszer összehívja az adatvédelmi tisztviselők konferenciáját.[196] Mindennek eredményeként pedig a jogi megfelelés mellett megvalósulhat a jogalkotói cél, a magánszféra védelmének magasabb szintje.

Statikussága nem jelenti azt, hogy ne lenne jelentős építőköve a védelemnek. Az ilyen komponenseknek különös szerepük van a „fordított gravitáció" megjelenítésében, ugyanis ezeknek a szabályozási pontoknak az ereje abban mutatkozik meg, hogy bevezetésük után a megszüntetésük nagyon nehezen támasztható alá érvekkel. Különösen akkor, ha az intézmény egyébként jól működik. A tisztviselői intézmény tehát egy stabil építőeleme a védelemnek, létezése önmagában sokat jelent a magánszféra védelmének érvényesítésében.

Az adatvédelmi tisztviselő kinevezésének kötelezettsége

A következőkben azt mutatom be, hogy hol és milyen feltételek fennállása esetén kell kinevezni adatvédelmi tisztviselőt. Azokban az esetekben, amikor nem nyilvánvaló, hogy az adatvédelmi tisztviselő kinevezése nem szükséges, a testület azt ajánlja, hogy az adatkezelő dokumentálja azt a mérlegelést, amely a kinevezés mellőzéséhez vezetett. Ez része a Rendeletnek való megfelelést bemutató dokumentációnak, amely adott esetben a felügyeleti hatósággal való kapcsolatban releváns lehet. Szükség esetén ezt a dokumentumot frissíteni kell, ha például az adatkezelő új tevékenységekbe kezd, amely már a kinevezés kötelezettségével járhat. Ez a követelmény az elszámoltathatóság elvéből fakad.

A kinevezési kötelezettség mindig olyan helyzetben jelenik meg, ahol a védelem megerősítésre, kiigazításra szorul. Egyfajta kompenzációként értékelhető, ahol a védelmi deficit megjelenik, vagy a kockázatok magasabb szinten határozhatók meg. A következőkben azt elemzem, hogy az adat-

[196] Infotv. 25/N. §.

védelmi tisztviselő jogalkotó által meghatározott szerepében milyen módon járulhat hozzá a védelem erősítéséhez. A testület kiemeli, hogy az adatvédelmi tisztviselők „közvetítő szerepet töltenek be az érdekelt felek (például a felügyeleti hatóságok, az érintettek és a szervezeten belüli részlegek) között”.[197]

A Rendelet először felsorolja azokat a szervezeteket, ahol ki kell nevezni tisztviselőt. Ilyen adatkezelő szervezetek a közhatalmi, illetve a közfeladatot ellátó szervek. Ezek definícióját nem uniós, hanem tagállami szinten kell megadni. A közhatalmi szervek magukban foglalják a központi, regionális és helyi kormányzati szerveket, a közfeladatot ellátó szervek pedig széles skálát jelentenek.

A testület véleménye a közfeladatot ellátó szervek között megemlíti a tömegközlekedési szolgáltatásokat, közszolgáltatásokat (víz és áram), közútfenntartás ellátóit, közszolgálati műsorszolgáltatókat, szabályozott szakmák fegyelmi testületeit. A vélemény szerint ezekben az esetekben is hasonló az érintett helyzete, mint a közhatalmi szervekénél, tehát nincs választása, hogy alanyává válik-e az adott jogviszonynak, illetve nincs befolyása az adatok kezelésére, ezért is indokolt az a pótlólagos védelem, amit a tisztviselő jelenthet. Jó gyakorlatként említi a vélemény azt, hogy azok a magánszervezetek, amelyek valamilyen közfeladatot is ellátnak kineveznek adatvédelmi tisztviselőt, és az ő tevékenységük kiterjed egyébként a nem közfeladathoz kötődő személyes adatkezelésekre is.

A Rendelet azután felsorol tevékenységeket, amelyek indokolják a tisztviselő kinevezését: fő tevékenységük rendszeres, szisztematikus és nagymértékű megfigyelést *(monitoring)* foglal magában. Itt nem csupán azokat a tevékenységeket kell érteni, amelyek a szó hétköznapi értelmében jelentenek megfigyelést (például kamerás megfigyelés), hanem a felhasználói magatartást nagy részletességgel rögzítő, naplózótevékenységeket is (például számlázási vagy bűnüldözési célból). Fontos, hogy ez a kitétel csak a magánszektorban működő adatkezelőkre vonatkozik, nem vonatkozik tehát a közszférára, mert ott egyébként általános kinevezési kötelezettség érvényesül. A kockázatalapú megközelítés itt is tetten érhető. Ott, ahol a közszféra körébe tartozó szervezetek kezelik a személyes adatokat, az adatvédelmi tisztviselő fontos garanciaként jelenik meg a jogszerűség fenntartása érdekében.

[197] Testületi iránymutatás az adatvédelmi tisztviselővel kapcsolatban, 5.

A 680/2016-os számú bűnügyi irányelv,[198] amely az adatvédelmi csomag része, szintén kötelezővé teszi az adatvédelmi tisztviselő kinevezését. Itt tehát a tevékenység jellege az a körülmény, amely a kinevezést indokolja.[199] A bűnügyi jellegű adatok kezelése mindig kiemelt kockázatnak tekintendő. Ez nem csupán az elkövetett bűncselekmények társadalmi súlyával magyarázható, hanem az érintettre a jogellenes adatkezelés következményei is sokkal súlyosabbak az általános adatkezelési kockázatoknál. Az adatvédelmi elvek és szabályok betartása ezen a területen tehát különös figyelmet érdemel.

Végül a Rendelet felsorolja azokat az adatokat, amelyeknek a kezelése, ha a fő tevékenységi körhöz tartozik, és nagy számban kezelnek ilyen adatokat, akkor a tisztviselő kinevezése kötelező: a különleges adatok[200] tartoznak ide, ahol a Rendelet külön kategóriaként határozza meg a büntetőjogi felelősséggel kapcsolatos adatokat.[201]

Figyelmet érdemel, hogy a Rendelet alkalmazásától kezdve olyan adatok is a különleges adatok körébe tartoznak immár, amelyek a Rendelet előtt még nem: ilyen a biometrikus és a genetikai adatok köre.

A Rendelet 9. cikke a „természetes személyek egyedi azonosítását célzó genetikai és biometrikus adatok" kezelését is a személyes adatok különleges kategóriájaként határozza meg. A technológia lehetővé teszi a biometrikus adatok tömeges és egyre biztonságosabb kezelését. A biometrikus adatok kezelése különös kockázatot jelent, hiszen az ilyen adatok nem változtathatók meg. Ha az érintett biometrikus adatainak mintáját megszerzik, onnantól kezdve ennek kezelése és esetleges jogellenes vagy véletlenszerű használata jelentős kockázatot jelent a magánszférára nézve. A biometrikus és a genetikai adatok kezelése során a *privacy by design* elve különös súllyal esik latba.

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

[199] A kötelezés általános, a Rendelet (97) preambulumbekezdése azonban a kinevezés kötelezettsége alól az eljáró bíróságokat és egyéb független igazságügyi hatóságokat felmenti.

[200] A Rendelet 9. cikkében meghatározott adatkör.

[201] A Rendelet 10. cikke külön szabályokat állapít meg a büntetőjogi felelősség megállapítására vonatkozó határozatokra és a bűncselekményekre vonatkozó személyes adatok kezelése terén.

Értelmezési kérdések

A kinevezési kötelezettség kapcsán több értelmezési kérdés is adódik, amelyekre a Rendelet alapján nem kapunk egzakt választ. Idetartozik a fő tevékenység, a nagymértékű adatkezelés, a rendszeres és szisztematikus adatkezelés megítélése, továbbá annak mérlegelése, hogy az adatkezelő vagy az adatfeldolgozó nevezi-e ki a tisztviselőt. A testület iránymutatása ezekben a kérdésekben még akkor is nyújt némi eligazítást, ha tudjuk, hogy a hatóságok teljesen egzakt válaszokat nem tudnak nyújtani, a gyakorlat ezeket a jogkérdéseket majd esetről esetre válaszolja meg.

Fő tevékenység

A Rendelet több ponton is utal a fő tevékenységre. A (97) preambulumbekezdés szerint az adatkezelők fő tevékenységi körébe az adatkezelők elsődleges tevékenységei tartoznak, a járulékos tevékenységként végzett személyes adatok kezelése nem.

A fő tevékenység kitétele mindig az adott kontextusban értelmezendő, és az adott adatkezelő szervezet elsődleges rendeltetése alapján ítélendő meg. Egy kórház esetében például a gyógyító-megelőző tevékenység a fő feladat, és mivel ezt személyes adatok tömege nélkül nem tudnák ellátni, ezért a kinevezés kötelezettsége itt is érvényesül. Egy magánbiztonsági cég nagy területen és sok személyt figyel meg – ebben az esetben is érvényesül, hogy fő tevékenysége együtt jár a személyes adatok kezelésével. Sportegyesület esetében a szurkolók beléptetése megint csak a fő tevékenységi körhöz tartozik. Hasonlóképpen a követeléskezelő szervezetek esetében az ügyfelekkel való kapcsolattartás, az ahhoz tartozó adatkezelés ismét fő tevékenységnek tekintendő. A NAIH egy eljárása során megállapította, hogy a szakszervezet tagjainak nyilvántartása nem járulékos, hanem fő tevékenységnek tekintendő. A skála másik oldalán olyan járulékos adatkezeléseket kell említeni, amelyek nem indokolják az adatvédelmi tisztviselő kinevezését, például sem a munkavállalói adatok kezelése a bérszámfejtés céljából, sem a szokásos IT-támogatási tevékenységek.

Nagymértékű adatkezelés

A Rendelet nem definiálja pontosan a nagymértékű kitételt, de a (91) preambulumbekezdés nyújt némi eligazítást. E szerint nagymértékű adatkezelésnek tekintendő az, amely jelentős mennyiségű személyes adat regionális, nemzeti vagy nemzetközi szintű kezelését célozza, továbbá amelyek az érintettek jelentős számára hatással lehetnek.

Nem lehet ezt a kritériumot teljes pontossággal meghatározni, a Testület mégis nyújt támpontokat ennek mérlegeléséhez: az adatalanyok száma, a kezelt adatok mértéke, az adatkezelés időtartama, tartóssága, az adatkezelés földrajzi kiterjedtsége mind figyelembe veendő.[202] Mindezek alapján a nagymértékű adatkezelés körébe tartozó adatkezelésnek tekintendő:

- egy kórház,
- illetve a közlekedési rendszerek adatkezelése (például elektronikus jegyeken keresztül),
- valós idejű helymeghatározó adatok kezelése adott (például nemzetközi élelmiszerlánc részéről),
- egy biztosító vagy bank ügyféladat-kezelése,
- a keresőmotor magatartás-alapú reklámozási tevékenysége,
- a telefon- vagy internetszolgáltató adatkezelése (tartalom, forgalom, helymeghatározás),
- egy nagy tömegrendezvény (a köznyelvben: fesztivál) kapcsán kezelt adatok tömeges mérete miatt, még akkor is, ha az adatkezelés rövid ideig valósul is meg.

Rendszeres és szisztematikus megfigyelés

Ezt a kitételt sem definiálja a Rendelet szövege, a (24) preambulumbekezdés említi a megfigyelést, igaz, más kontextusban. E szerint annak meghatározásakor, hogy az adatkezelés az érintett magatartása megfigyelésének minősül-e, meg kell vizsgálni, hogy a természetes személyeket nyomon követik-e az interneten, illetve ezután az érintett profiljának elkészítését is magában foglaló adatkezelést alkalmaznak-e annak érdekében, hogy a természetes személyre vonatkozó döntéseket hozzanak, vagy elemez-

[202] Lásd A személy- és vagyonvédelmi, valamint a magánnyomozói tevékenység szabályairól szóló 2005. évi CXXXIII. törvény 72/C. §-át.

zék, illetve előre jelezzék a személy preferenciáit, magatartását vagy éppen beállítottságát.

Az internetes követés és profilozás egyértelműen rendszeres és szisztematikus megfigyelésnek minősül, amelybe beleértjük a magatartásalapú reklámozást is.[203] Az internet csak egy példa, minden más közegben megvalósuló rendszeres és szisztematikus megfigyelés kiváltja a tisztviselő kinevezési kötelezettségét. A profil elkészítése privacyszempontból mindig fokozott kockázatot jelent, hiszen a profilozás révén nem csupán a múltbeli, hanem a jövőbeli viselkedésre nézve is pontos becslést lehet megadni. Az ilyen jellegű adatkezelés a magánszférába fokozott beavatkozást jelent.

Az adatkezelőnek vagy az adatfeldolgozónak kell kineveznie az adatvédelmi tisztviselőt?

A feltett kérdésre nincs általános válasz, de mintha az adatkezelőnél természetesebben adódna a kinevezési kötelezettség, mint az adatfeldolgozónál.[204] Az, hogy az adatkezelőnél ki kell nevezni tisztviselőt, nem jár automatikusan kinevezési kötelezettséggel az adatfeldolgozó oldalán. Elképzelhető olyan eset, amikor az adatkezelőre nem, de az adatfeldolgozóra vonatkoznak már a tárgyalt kritériumok, ezért ott kötelező lesz a kinevezés.[205]

A testület példája a következő: egy családi vállalkozás kiskereskedelemmel foglalkozik, amely nem jár nagymértékű adatkezeléssel. Azonban előfordulhat, hogy az adatfeldolgozó, amely számos üzleti szereplőt kiszolgál honlapok elemzése és célzott reklámozás révén, már olyan mennyiségű adatot kezel, amely teljesíti a nagymértékű kitételt. Ebben az esetben az adatfeldolgozónak ki kell jelölnie adatvédelmi felelőst, míg az adatkezelő mentesül ez alól.

[203] Lásd *Testületi iránymutatás az adatvédelmi tisztviselővel kapcsolatban,* 11. A testület ezen a ponton számos példát említ még.

[204] A Rendelet 4. cikk 8. pontja szerint az adatfeldolgozó az a természetes vagy jogi személy, közhatalmi szerv, ügynökség vagy bármely egyéb szerv, amely az adatkezelő nevében személyes adatokat kezel.

[205] *Testületi iránymutatás az adatvédelmi tisztviselővel kapcsolatban,* 11–12.

A kinevezési kötelezettség köre a védelmi lépcső fényében

Amint utaltam rá, a tisztviselői kinevezés kötelezettsége a kockázattal arányos, illetve a védelmi deficit kompenzálására szolgál. Ez a Rendelet szabályozási koncepciója. Ez a koncepció markánsan különbözik a korábbi adatvédelmi irányelvi szabálytól, amely gyakorlatilag a tagállamokra bízta a kinevezés mérlegelését. Nem különbözik azonban jelentősen attól a szabályozási koncepciótól, ami a magyar Infotv.-ben, vagy éppen az uniós intézményekre vonatkozóan már a 2001-es rendeletben megjelent. Ilyen értelemben a Rendelet bár a védelmi lépcsőn előrelépésként azonosítható, leginkább egy jogalkotási mulasztás korrigálásáról van szó. Ez nem vesz el a jogalkotás értékéből, mégis megemlítendőnek tartom, hogy ebben a tekintetben nem az uniós, hanem a tagállami jogalkotó járt elöl jó példával, és mutatta meg a helyes irányt az uniós jogalkotó számára.

Az első két lépcső azonosítása után kísérletet teszek a harmadik szint meghatározására. A jelenleginél magasabb védelmet biztosítani hivatott fok jellemzője továbbra is a kockázatalapú megközelítés. Az a szabályozás megőrzendő eleme, hogy a közszférában, továbbá azokban a jogviszonyokban, ahol nem az érintett választásán múlik a jogviszonyba való belépés, vagy az onnan való kilépés, kötelező a tisztviselő kinevezése.

A szabályozásnak teret kellene ugyanakkor nyújtania abban, hogy a jogalkotótól függetlenül az általános szabályokat kiigazíthassák. Az adatvédelmi felügyeleti hatóságokat tömörítő testületet olyan szabályozási funkcióval kellene felruházni, amelynek révén a kinevezési kötelezettség szükséges módosításai elvégezhetők. Ez gyakorlatilag egyfajta delegált jogalkotás lenne, és a Rendelethez kapcsolódó „végrehajtási rendeletként" funkcionálna. Ez garantálná azt, hogy a nehézkesen alakítható jogszabályi követelmények valóban a napi gyakorlatban megmutatkozó kockázatokhoz legyenek igazíthatók.

Ezeket a kockázatokat pedig a hatósági gyakorlat nagyon pontosan meg tudja mutatni. A Rendelet alkalmazásának első két évében például kirajzolódott, hogy a határon átnyúló adatkezelések esetében nehézkes az érintetti joggyakorlás. Az egyablakos ügyintézés az adatkezelő számára kézenfekvő eljárási keretet nyújt, az érintett azonban jól kitapinthatóan nehezebb eljárási pozíciót foglal el a rendeleti szabályozást megelőzővel összevetve.
Az unión belül határon átnyúló adatkezeléseken túl az unión kívüli dimenzió még több eljárási kérdést vet fel. Ezekben az esetekben ugyan nem érvényesül

az egyablakos ügyintézés, de a hatóságok jogérvényesítési lehetőségeinek korlátai jól láthatók. Ilyen esetekben például a tisztviselő kinevezési kötelezettsége a védelmi deficit orvoslásának egyik lehetséges eszközeként jelenik meg.

Ez annál is indokoltabb, mivel nemcsak a magánszférát érintő adatkezelési célok bővülnek gyorsan, hanem az üzleti modellek, a fogyasztói magatartás is változik. A tisztviselői kinevezést bizonyos esetekben kötelezővé kell tenni, ha a körülmények indokolják, ezt pedig véleményem szerint gyorsan és a szükséges szakértelem birtokában a testület hivatott megtenni.

A tisztviselői intézmény még tudatosabb alkalmazását jelentené, ha az adatvédelmi felügyeleti hatóság határozatában elrendelhetné, mintegy pótlólagos védelmi intézkedésként, hogy a vizsgálat alá vont szervezet nevezzen ki adatvédelmi tisztviselőt meghatározott időre. Ez az arányosságot igénylő intézkedés hozzájárulhatna ahhoz, hogy a tisztviselői intézmény még inkább gyökeret verjen a napi gyakorlatban, és a hatóságok ilyen módon is elősegíthessék a jogszabályoknak való megfelelés kikényszerítését.

Az adatvédelmi tisztviselő feladatai és jogállása

A Rendelet a tisztviselővel szemben, annak kinevezése előtt támasztott követelmények között a szakmai rátermettségéről és a feladatai ellátására való alkalmasságáról rendelkezik. Az adatvédelmi jogot és gyakorlatot szakértői szinten ismerő személy nevezhető ki vagy bízható meg.

A Rendelet az adatkezelések egy részének természetéből adódóan nemzetközi közegben érvényesítendő, ezért külföldi munkavállalókra is alkalmazhatók, ezt a jogszabály nem tiltja. A Rendelet rugalmas szabályai lehetőséget adnak arra, hogy a széles személyi körből válogatva a leginkább rátermettet választhassák ki a feladatra, ezáltal is elősegítve az adatvédelem erősítését a szervezeten belül.

A Rendelet szerint az adatkezelés sajátosságai és a kezelt adatok számára az adott körülmények között nyújtandó védelem alapján ítélendő meg, hogy milyen ismeretek szükségesek. A felkészültséget illetően ugyanakkor meglehetősen konkrét elvárásokat is említ a Rendelet: az Európai Unió és az adott ország adatvédelmi jogának és gyakorlatának szakértői szintű ismerete elvárás. Mind a munkáltatónak, mind a tisztviselőnek fontos tájékozódási pontot nyújtana, ha erről valaki igazolást tudna bemutatni, és erre van is igény.

A felkészültség kapcsán hivatkozhatunk az Európai Adatvédelmi Biztos 2010-ben kibocsátott elemzésére,[206] amelyben az uniós intézmények által kinevezett adatvédelmi tisztviselőkkel kapcsolatos szabályokról ad tájékoztatást.[207] Ez a dokumentum öt konkrét képzettséget említ, nevezetesen a CIPP-,[208] a CIPP/IT-,[209] továbbá a CISSP-,[210] a CISA-[211] és a CISM-[212] képzéseket. A 2010-es dokumentum kibocsátását követően nyílt meg a CIPP/E-képzés,[213] amely kifejezetten az európai adatvédelmi jogra fókuszál a bemutatott képzéscsaládon belül. Az európai adatvédelmi biztos álláspontja szerint ezek megléte fontos szempont az uniós intézménynél dolgozó tisztviselő kiválasztása során.

Az Európai Adatvédelmi Biztos dokumentuma nem az általános adatvédelmi Rendelet értelmezése céljából készült, továbbá csupán egyetlen szervezet képzéseit említi. A megszerezhető képzettségek és képesítések országonként változók lehetnek. Magyarországon jelenleg már egyetemen képeznek adatvédelmi szakértőket, illetve adatvédelmi szakembereket.

Bizonyos értelemben érzékeny vagy nehezen megragadható kritérium az alkalmasság. A testület megpróbált ezen a téren is tájékozódási pontokat kijelölni, ilyenek mindenekelőtt a személyes képességek, úgymint az integritás, amely a szervezet integritásának, értékeinek védelme érdekében nélkülözhetetlen, továbbá a magas szintű szakmai etikai elvárások vagy a diszkréció.[214] Mindezek alapvetőek akkor, amikor az az elvárás

[206] Az Európai Adatvédelmi Biztos által 2010. október 14-én nyilvánosságra hozott dokumentuma: Professional Standards for Data Protection Officers of the EU Institutions and Bodies Working Under Regulation (EC) 45/2001. *Ec.europa.eu.*

[207] Az Európai Parlament és a Tanács 45/2001/EK Rendelete (2000. december 18.) a személyes adatok közösségi intézmények és szervek által történő feldolgozása tekintetében az egyének védelméről, valamint az ilyen adatok szabad áramlásáról három-, illetve hétéves szakmai tapasztalatot vár el a kinevezett tisztviselőktől.

[208] Certified Information Privacy Professional.

[209] Certified Information Privacy Professional/Information Technology.

[210] Certified Information Systems Security Professional.

[211] Certified Information System Auditor.

[212] Certified Information Security Manager.

[213] Certified Information Privacy Professional/Europe.

[214] Lásd *Testületi iránymutatás az adatvédelmi tisztviselővel kapcsolatban,* 14.

a tisztviselővel szemben, hogy a szervezeten belül az adatvédelmi kultúra kialakulását, megerősítését segítse elő.

További lehetséges kritériumként említhető az együttműködés képessége és a megbízhatóság. A megbízhatóság az összeférhetetlenséggel is szoros összefüggést mutat, és az összeférhetetlenséget – az adott tisztviselő hozzáállásától vagy személyes kvalitásaitól függetlenül – vélelmezni kell a következő személyek esetében: a tulajdonos, a vezető testület tagja, egyéb magas rangú vezető, a betöltött munkakör okán össze nem egyeztethető feladatok ellátói (informatikai vagy humánerőforrás-vezető, a napi adatkezelési feladatokat irányító munkatársak), továbbá a felsorolt személyek közeli hozzátartozói.[215]

A foglalkoztatás szabályai

A foglalkoztatást illetően a Rendelet rugalmasságra törekszik. A vállalkozáscsoport közös tisztviselőt is kijelölhet, ha a tisztviselő könnyen elérhető. Az elérhetőség kapcsán nyilvánvalóan a nemzetközi működés sajátosságait is figyelembe kell venni, de mindenképpen szükség van helyben is személyzetre, hiszen a helyi viszonyok ismerete nélkülözhetetlen, az adatalanyokkal való kapcsolattartás pedig például nyelvismeret nélkül nem képzelhető el. A közelség és az elérhetőség tehát meghatározó elvárás. A testület szerint elsőbbséget élvez az a megoldás, hogy a tisztviselő az Európai Unióban működik, de elismeri, hogy lehetnek olyan esetek, amikor hatékonyabban láthatja el a feladatát egy harmadik országban tevékenykedve. Az adott szervezet, illetve az érintettek igényeire kell tekintettel lenni ennek mérlegelésekor.

A foglalkoztatás formáját illetően a Rendelet szerint a tisztviselő lehet alkalmazott, vagy szolgáltatási szerződés, tehát munkaviszony vagy megbízás keretében is elláthatja a feladatát.

[215] A bajor adatvédelmi hatóság 2016. október 20-án nyilvánosságra hozott közleménye szerint a jogsértés miatt szükségesnek látta pénzbírság kiszabását. Forrás: a Bayerisches Landesamt für Datenschutzaufsich honlapja (Pressemitteilung: Datenschutzbeauftragter darf keinen Interressenkonflikten unterliegen).

A tisztviselő adatainak nyilvánossága, elérhetőség

A jogállás fontos jellemzője a nyilvánosság, tehát bárki által megismerhető információ a név és az elérhetőség. Ezt a hatóság nyilván is tartja. A nyilvánosságnak természetesen garanciális jelentősége is van, hogy esetleges panasz esetén a tisztviselő bárki számára elérhető legyen.[216]

A külvilág felé történő nyilvánosságra hozatal mellett meg kell említeni a belső nyilvánosságot, amely azt szolgálja, hogy a szervezet munkavállalói személyesen el tudják érni a tisztviselőt. Az is alapvető elvárás, hogy a szervezet munkavállalói bizalommal kereshessék a tisztviselőt, ezért írja elő a Rendelet a tisztviselő számára a titoktartási kötelezettséget, illetve az adatok bizalmas kezelésére vonatkozó kötelezettséget.[217]

A panaszon túl a Rendelet az érintettek számára kötelezően elérhetővé rendeli a tisztviselőt akkor, amikor a személyes adataik kezeléséhez és jogaik gyakorlásához kapcsolódóan bármilyen kérdést megfogalmaznak. Ez nem jelenti azt, hogy a tisztviselő a kizárólagos kapcsolattartó adatvédelmi ügyekben, de neki kötelessége az adatalanyok rendelkezésére állni, különösen például adatvédelmi incidensek esetében. Ez lehet e-mail, telefonvonal, meg lehet könnyíteni a kapcsolatba lépést továbbá egy webes formula kialakításával is.

Teljes vagy részmunkaidős foglalkoztatás

A tisztviselőnek nem kell teljes állásban ezt a feladatát betöltenie, illetve egy személy több szervezetnél is elláthat ilyen feladatokat. Sőt elképzelhető az is, hogy egy csoport látja el a tisztviselői feladatokat, elismeri a testület ugyanis, hogy ez hozzájárulhat a tevékenység magasabb szintű ellátásához. Ilyen esetben azonban ki kell jelölni azt a személyt a csoportból, aki valóban felelős az adott szervezet vonatkozásában, a tisztviselői tevékenység tehát nem válhat személytelenné. A szabályozás szelleme és logikája azt mutatja,

[216] Az eredeti angol verzió nem említi a tisztviselő nevét, míg a magyar verzió már igen (contact details – nevét és elérhetőségét), mint nyilvános, valamint a hatósággal közlendő adatot. Érdekes módon a bűnügyi irányelv magyar verziója ugyanezzel a fordítási hibával jelent meg a hivatalos közlönyben. Az érintettnek a Rendelet 13. és 14. cikke alapján nyújtandó tájékoztatásnak szintén része az adatvédelmi tisztviselő elérhetősége.

[217] Lásd *Testületi iránymutatás az adatvédelmi tisztviselővel kapcsolatban,* 15.

hogy személyes közreműködésről, függetlenségről és végső soron felelősségről van szó, amelynek címzettje egy természetes személy kell hogy legyen.

A felügyeleti hatóság feladatai kapcsán a Rendelet is és az irányelv is előírja, hogy azok ellátása az érintett és az adatvédelmi tisztviselő számára térítésmentes legyen.[218]

Az adatkezelő feladatai a tisztviselő munkájának támogatása terén

Az adatkezelő vagy adatfeldolgozó (a foglalkoztató) az adatvédelmi tisztviselőt megfelelő forrásokkal támogatja, hogy feladatait el tudja látni. Ez magában foglalja a szükséges anyagi forrás, megfelelő helyiség, szükség esetén munkatársak rendelkezésre bocsátását. Azt is biztosítani kell, hogy a személyes adatokhoz, valamint az adatkezelési műveletekhez (ezek megtekintéséhez, megfigyeléséhez) legyen hozzáférése.[219] A 30. cikk szerinti nyilvántartás ebből a szempontból kulcsfontosságú, ezért javasolható a tisztviselőknek, hogy ezt a feladatot személyesen ők lássák el. A tisztviselő e nyilvántartás vezetése révén teljes rálátást nyer a szervezeten belül zajló adatkezelésekre.

A Rendeletet megelőző szabályozás idején az adatvédelmi hatóság tartott számot arra, hogy az adatkezelésekre teljes rálátással bírjon. Kétségtelen, hogy voltak kivételek ez alól, de a fő szabály a bejelentési kötelezettség volt. Különösen markáns volt ez az elvárás az Egyesült Királyságban, ahol a bejelentési kötelezettség elmulasztása az adatkezelés tilalmával járt.[220]

A nyilvántartást rendszeresen frissíteni kell, a frissítés tényét pedig a nyilvántartást vezető tisztviselőnek kell bejelenteni. Ez a szerep egyfajta kontrollal jár. E nyilvántartás vezetése olyan feladat, amely álláspontom szerint összeegyeztethető a tisztviselő független szerepével és nem vezet feladatok közötti konfliktushoz.

További kötelezettség a foglalkoztató oldalán, hogy biztosítja a tisztviselő számára azokat a forrásokat, amelyek szakértői szintű ismereteinek

[218] A Rendelet 57. cikk (3) bekezdése, illetve az irányelv 46. cikk (3) bekezdése szerint.
[219] Lásd *Testületi iránymutatás az adatvédelmi tisztviselővel kapcsolatban,* 17.
[220] Vö. Peter Carey: *Data Protection – A Practical Guide to UK and EU Law*. New York, Oxford University Press Inc., 2009. 28–29.

fenntartásához szükségesek. Ezek meglehetősen konkrét elvárások, amelyekből adódik például a munkaidőn belül a továbbképzés feltételeinek megteremtése is. Jóri és szerzőtársai szerint ez magában foglal egy olyan saját költségvetést, amelyből a képzés és továbbképzés feltételei megteremthetők.[221]

Az adatkezelő feladata annak szavatolása, hogy a tisztviselő a feladatait és kötelezettségeit függetlenül tudja ellátni. A tisztviselő függetlenül látja el tehát a feladatait, ez azonban nem jelent felelőtlenséget. A függetlenség azt jelenti, hogy nem fogadhat el senkitől sem utasítást, ennek garantálása az adatkezelő szervezet kötelezettsége. Adatvédelmi ellenőrzési feladatai terén, a jogszerűség megítélése kapcsán tehát még a szervezeten belül sem utasíthatja senki. Nem utasíthatják arra, hogy miként kezeljen egy ügyet, milyen eredményre kell jutni, hogyan vizsgáljon ki egy panaszt, vagy éppen milyen jogértelmezést tegyen magáévá. Mivel az adatkezelés jogszerűségéért az adatkezelő felelős, ezért fontos, hogy a tisztviselő eltérő véleményét hangoztathassa a legmagasabb döntéshozatali fórum előtt is. Lehetővé kell tenni, és ez is egy jó gyakorlat, hogy a tisztviselő évente beszámoljon tevékenységéről a legfelső menedzsmentnek.[222]

Munkajogilag is értelmezhető védettséget jelent a számára, hogy feladatai ellátásával összefüggésben nem bocsátható el, de még csak szankcióval sem sújtható. A szankció természetesen tágan értelmezendő, és minden, egyébként járó előny elmaradása is szankciónak tekintendő, amennyiben az a feladatai ellátásával összefüggést mutat. Ilyen lehet például az előmenetel hátráltatása, a többi munkavállalónak járó előnytől való megfosztás. Mivel kényes egyensúlyról van szó, ezért nem csupán a bekövetkezett hátrányok minősülnek jogellenesnek, hanem az ezzel való fenyegetés is, amennyiben az a tisztviselő munkájának befolyásolására irányul.

A nemzetközi gyakorlatban merült fel az a kérdés, hogy a Rendelettel összeegyeztethető-e az a munkaszerződésbe foglalt kikötés, amely szerint az adatvédelmi tisztviselőnek meg kell térítenie az adatvédelmi bírságot, amennyiben rossz tanácsot ad az adatkezelő szervezetnek. Az ilyen megoldás több okból is jogellenes álláspontunk szerint. Az adatvédelmi tisztviselő ugyanis nem hoz döntéseket az adatkezelést illetően, ennek megfelelően az általa meg nem hozott döntésekért sem tehető felelőssé. Másrészt egy

[221] E költségvetésből kell tudni fedezni a szakkönyvek vásárlását, konferenciákon való részvételt. Jóri András et al.: *A GDPR magyarázata*. Budapest, HVG-ORAC, 2018. 321.
[222] Lásd *Testületi iránymutatás az adatvédelmi tisztviselővel kapcsolatban,* 16.

ilyen kikötés olyan nyomás alá helyezné a tisztviselőt, amelyből a biztonságot keresve, a felső vezetői akarattal konform véleményt alakítana ki, kerülve az esetleges jogsértésből eredő kockázatokat, illetve a menedzsment akaratához igazítaná tanácsainak tartalmát. Ilyen körülmények között a tisztviselő nem tudja feladatait a Rendeletben megfogalmazott módon ellátni.

Természetesen vannak esetek, amikor a tisztviselő jogviszonya jogszerűen szüntethető meg. A testület példájánál maradva ilyen lehet, amikor a tisztviselőt lopáson érik, vagy pszichésen, fizikailag, vagy akár szexuálisan zaklatja munkatársait, vagy hasonló súlyos visszaélést követ el.[223] A munkavégzése során megvalósuló súlyos mulasztások szintén járhatnak a tisztviselő felmentésével.

A tisztviselő megbízásával kapcsolatban a jogalkotó nem várja el a határozatlan idejű kinevezést. A munkajogi szabályokkal összhangban álló határozott idejű kinevezés meg nem újítása szankcióként is értelmezhető, ugyanakkor álláspontom szerint a szerződés határozott idő lejártát követő meg nem újítása jogszerű megoldás lehet olyan esetekben, amikor a megbízó adatkezelő vagy adatfeldolgozó jogszerűen kíván a korábbi tisztviselő helyett mást foglalkoztatni.

Nem hozott változást a Rendelet azon a magyar jogban már ismert szabályozáson, hogy a tisztviselő a szervezet legfelső vezetésének tartozik felelősséggel. Feladatai ellátásához nélkülözhetetlen a vezetői szintű támogatás. Bármilyen munkakör ellátását el lehet ugyanis lehetetleníteni azzal, ha egyszerűen nem hagynak rá időt, ezért a tisztviselő esetében is elvárás és testületi ajánlás a megfelelő idő biztosítása. Jó gyakorlat, ha százalékosan határozzák meg a tisztviselői feladatokra fordítható idő mennyiségét. Ha szükséges, akkor további munkavállalókat kell a tisztviselő rendelkezésére bocsátani, hogy feladatait hatékonyan el tudja látni.[224]

A tisztviselő munkájának támogatása körében említendő még a házon belüli szolgáltatásokhoz való hozzáférés, úgymint a HR-, a jogi, a biztonsági, az IT-terület annak érdekében, hogy támogatást, a közös feladatokhoz segítséget, továbbá információkat kaphasson.[225]

[223] *Testületi iránymutatás az adatvédelmi tisztviselővel kapcsolatban,* 18.
[224] Lásd *Testületi iránymutatás az adatvédelmi tisztviselővel kapcsolatban,* 17.
[225] *Testületi iránymutatás az adatvédelmi tisztviselővel kapcsolatban,* 17.

Összeférhetetlenség

Ha több feladatot is ellát a tisztviselő, tehát tisztviselői feladatai mellett egyéb kötelezettségei is vannak, akkor az adatkezelőnek kell biztosítani azt, hogy ezekből a feladatokból ne fakadjon összeférhetetlenség. Első helyen kell említeni azokat a munkaköröket és feladatokat, ahol a tisztviselőnek például az adatkezelés célját és eszközeit illetően kellene döntést hoznia. Ezek mindenképpen összeférhetetlenek a független tanácsadói, megfigyelői, illetve ellenőrző funkciójával. Ennek megfelelően nem lehet például ügyvezetői pozícióban, vagy HR-, esetleg IT-vezető. Szintén konfliktust eredményezhet, ha a tisztviselőt azzal bízzák meg, hogy a szervezetet képviselje a bíróság előtti eljárásban, és ilyen módon abba a helyzetbe kerül, hogy az adatkezelő álláspontját a saját meggyőződésétől függetlenül kell képviselnie.[226] Jó gyakorlat, ha az összeférhetetlenség érdekében megfogalmazott elvárásokat belső szabályzatban rögzítik.

A bajor adatvédelmi biztos 2016 októberében nyilvánosságra hozott közleményében[227] mutatott be egy olyan ügyet, amelyben az adatkezelő szervezet a tisztviselőre vonatkozó összeférhetetlenségi szabályokat szegte meg. A vonatkozó, a Rendeletet megelőzően már alkalmazandó szabályok szerint azon szervezetek, amelyek a személyes adatok automatikus feldolgozása területén legalább tíz főt foglalkoztatnak, kötelesek adatvédelmi tisztviselőt kinevezni. A bajor hatósági álláspont kiemelte, hogy ha valakit erre a pozícióra kineveztek, akkor nem kaphat olyan feladatokat, amelyek a tisztviselői funkcióval konfliktust eredményezhetnek. Ilyen konfliktus és összeférhetetlenség áll fenn, ha a tisztviselő egyúttal IT-vezető is a szervezetnél. Ebben az esetben ugyanis a tisztviselő nem tudja az adatvédelmi ellenőrző szerepét függetlenül ellátni, hiszen ilyenkor a saját munkáját kellene ellenőriznie. A tisztviselői feladattal összeegyeztethetetlen az adatkezelést érintő döntések meghozatala, illetve az ezekért viselt felelősség.

Mindennek megfelelően azon szervezetek, amelyek adatvédelmi tisztviselő kinevezésére kötelesek, csak olyan személyt nevezhetnek ki, aki ezt a feladatát el tudja látni minden külső befolyás nélkül. Azok a szervezetek pedig, amelyek ismételt felhívás ellenére sem tesznek eleget e kötelezett-

[226] *Testületi iránymutatás az adatvédelmi tisztviselővel kapcsolatban,* 19.

[227] A bajor adatvédelmi hatóság 2016. október 20-án nyilvánosságra hozott közleménye szerint a jogsértés miatt szükségesnek látta pénzbírság kiszabását.

ségüknek, szükségszerűen pénzbüntetéssel kell hogy számoljanak a bajor hatóság közleménye szerint.

Bár a leírt eset a német (bajor) jog alapján ítélendő meg, a Rendelet is a szankcionálandó mulasztások között említi az adatvédelmi tisztviselőre vonatkozó kötelezettségeket.

> A Rendelet 83. cikk (4) bekezdésének a) pontja szerint az adatvédelmi tisztviselőre vonatkozó kötelezettségek megsértése esetén az adatkezelő, illetve az adatfeldolgozó legfeljebb 10 millió euró összegű közigazgatási bírsággal, illetve a vállalkozások esetében az előző pénzügyi év teljes éves világpiaci forgalmának legfeljebb 2%-át kitevő összeggel sújtható (a kettő közül a magasabb összeget kell alkalmazni).

Ennek megfelelően az adatvédelmi felügyeleti hatóságok hasonló ügyeket a Rendelet alatt is a bajor példához hasonlóan ítélnek meg. A hamburgi adatvédelmi hatóság egy olyan ügyben is pénzügyi szankciót alkalmazott, amikor ugyan volt kinevezett tisztviselő, de a kötelezően megadandó adatait nem juttatták el az illetékes hatósághoz.[228]

Az adatvédelmi tisztviselő feladatai – tanácsadás, ellenőrzés, kapcsolattartás

Minden adatvédelmi ügybe be kell vonni a tisztviselőt, méghozzá megfelelő időben. Nem választható el ez a rendelkezés a beépített adatvédelem elvétől, kellő időben és a folyamat kialakítása során nem túl későn kell az érdemi véleménynyilvánítást lehetővé tenni. A Rendelet sok ponton tesz említést a kockázatokról, a tisztviselő is köteles az adatkezeléssel együtt járó, az érintettek helyzetére vonatkozó kockázatokra tekintettel végezni a munkáját.

Az adatvédelmi tisztviselő a jogszabályokról és azok alkalmazásához kapcsolódó kötelezettségekről tanácsot ad az adatkezelőnek és az alkalmazottainak. Ellenőrzi a jogszabályoknak és a belső szabályoknak való megfelelést a személyes adatok kezelése terén. További feladata annak ellenőrzése, hogy a személyzet megfelelő adatvédelmi tudatossággal látja-e el

[228] A Facebook hamburgi leányvállalatát 51 ezer euró büntetéssel sújtotta a hamburgi hatóság ezért a mulasztásért: *28. Tätigkeitsbericht Datenschutz des Hamburgischen Beauftragten für Datenschutz und Informationsfreiheit 2019.* 105–107. Forrás: a hamburgi adatvédelmi hatóság honlapja.

tevékenységét, továbbá ellenőrzi a képzést is. Ezeken túl az úgynevezett kapcsolódó auditokat is ellenőrizheti. A tisztviselő tanácsot ad az előzetes adatvédelmi hatásvizsgálat során, és figyelemmel kíséri a hatásvizsgálat elvégzését.

Nevesített feladata a hatósággal való együttműködés, az előzetes adatvédelmi hatásvizsgálat kapcsán ő a kapcsolattartó a hatóság felé, és bármilyen adódó ügyben konzultációt folytathat a hatósággal. Abban, hogy kapcsolatba lép-e a hatósággal, nem adható neki utasítás, ebben a tekintetben a titoktartás nem akadályozhatja meg őt.[229] Jóri és szerzőtársai jó gyakorlatnak tekintik, ha a hatósággal munkakapcsolatot alakít ki a *„hatékony és gyors ügyintézés érdekében"*.[230]

A testület jó gyakorlatként javasolja, hogy a tisztviselőt a vezetői megbeszélésekre rendszeresen hívják meg. Ha bármilyen fórumon adatvédelmet is érintő döntést hoznak, a tisztviselő jelenléte kívánatos. Helyes gyakorlat, ha a szervezet azokban az esetekben, amikor nem követi a tisztviselő tanácsait, rögzíti, hogy ezt miért nem teszi.[231]

Bármilyen incidens, így adatvédelmi incidens esetén javasolt azonnal konzultációt kezdeményezni a tisztviselővel. Szintén érdemes a szervezet adatvédelmi szabályaiban meghatározni, hogy mikor kötelező a tisztviselővel konzultálni. Mind a Rendelet, mind az irányelv a hatósággal közlendő információk között említi a tisztviselő nevét és elérhetőségét.[232]

A tisztviselő feladatai az adatvédelmi hatásvizsgálat kapcsán

A tisztviselő az adatkezelő kérésére szakmai tanácsot ad az adatvédelmi hatásvizsgálatra vonatkozóan, illetve nyomon követi annak elvégzését. Ha van kinevezett tisztviselő, őt az adatkezelő köteles bevonni. Ha az adatkezelő szervezet nem tisztviselőt, hanem adatvédelmi tanácsadót foglalkoztat, mert nem terheli a tisztviselő kinevezésének kötelezettsége, akkor az ő bevonása nem kötelező.

[229] *Testületi iránymutatás az adatvédelmi tisztviselővel kapcsolatban,* 21.
[230] Jóri et al. (2018): i. m. 322.
[231] *Testületi iránymutatás az adatvédelmi tisztviselővel kapcsolatban,* 16.
[232] Az Európai Unió Hivatalos Közlönyében a Rendelet magyar verziója a „nevét és elérhetőségét" szöveggel került nyilvánosságra, míg az irányadó, a jogalkotás során használt angol nyelvű változat szerint „contact details of the data protection officer" szerepel (37. cikk [7] bekezdés).

A testület szerint a tisztviselő bevonása magában foglalja a tisztviselő részvételével annak mérlegelését, hogy el kell-e végezni a hatásvizsgálatot, milyen módszertan szerint tegyék ezt, házon belüli vagy külsős szereplők bevonásával történjen-e, milyen intézkedéseket kell tenni a kockázatok mérséklése érdekében, végül annak értékelését, hogy a hatásvizsgálatot helyesen hajtották-e végre, és annak eredménye a Rendelettel összhangban van-e.[233]

Az ajánlás szerint a hatásvizsgálattal összefüggő dokumentációnak része annak bemutatása, ha a tisztviselő javaslatától eltértek.

Összegzés

Az adatvédelmi tisztviselők a Rendeletnek való megfelelés érdekében jelentős és szerteágazó feladatokat látnak el. A bemutatott szabályok alapján jól látható, hogy munkájuk sok téren európai, illetve globális keretek között mozog, ezért is fontos a felkészültségük, folyamatos képzésük. Mindezek hozzájárulnak ahhoz, hogy az adatvédelmi tisztviselők a Rendelet alatti intézményrendszer fontos szereplőivé váljanak, így erősítve az adatkezelő szervezetekkel való együttműködésükben a jogbiztonságot, az adatalanyokkal való kapcsolataikban pedig a hatékony jogérvényesítést.

Az adatvédelmi tisztviselő feladatai és jogállása a védelmi lépcső elméletének fényében

A bemutatott tisztviselői feladatok és jogállás nem hasonlítható össze a korábbi, az adatvédelmi irányelvi helyzettel, hiszen akkor nem létezett kötelező kinevezés. Ezért ebben a tekintetben a védelmi lépcsőn csak két fokozatot tudunk azonosítani: a jelenlegit és a következőt, amely a kívánt irányt, a védelmet erősítő következő fok.

A védelmi deficitről korábban már részletesen szóltam. Annak felidézésére, hogy milyen fontosságú ügy letéteményese a tisztviselő, elég utalni Joshua és Christoph értékelésére, amely szerint az adatok nagy koncentrációja, amelyet „az idők során sok különböző forrásból építettek fel", a jólétet rongáló hatást gyakorolhat.[234] A tisztviselői szerep pont ennek a piaci

[233] *Testületi iránymutatás az adatvédelmi tisztviselővel kapcsolatban,* 20.
[234] Fairfield–Engel (2015): i. m. 385–399.

logikából adódó nehézkedésnek az ellensúlyozására szolgál. Olyan garancia, amely a látencia ellen, az átláthatatlanság ellen irányul.

Álláspontom szerint az adatvédelmi tisztviselői pozíciót tovább kell erősíteni, professzionalizálni szükséges, és egy sokkal kötöttebb rendben kell elfoglalnia a helyét az adatkezelő szervezeten belül. Bár a jogalkotás látszólag ebbe az irányba mutat, határozottabb lépésekre van szükség, és a rendeleti szabályokat egy ilyen jellegű módosításnak kell követnie minél hamarabb.

A kinevezési kötelezettség terjedelmével a tisztviselői intézmény léte kapcsán már szóltam. A kvázi végrehajtási rendeleti szabályozás révén bővíthető a kinevezési kötelezettség alá eső adatkezelők köre. A védelem erősítése akkor várható, ha annak személyi, intézményi, eljárási feltételei adottak.

Ami a személyi feltételeket illeti, a tisztviselő végzettségét előzetesen nem tartom vizsgálandónak, azonban egy uniós akkreditációjú vizsga előírása fontos garanciaként szolgálhatna. Ezt uniószerte meg lehetne szervezni, és ilyen módon szavatolni, hogy a tisztviselők felkészültsége megfelelő legyen. A vizsgán túl egyfajta kamarai tagságot is előírhatónak tartok. Ennek feltételei az Európai Gazdasági Térségben megteremthetők.

A személyes rendelkezésre állás az előírt vizsga és a kamarai tagság révén erősíthető. Ezt szükségesnek tartom annak érdekében, hogy a tisztviselői munkáért vállalt felelősség ne váljon szétporlaszthatóvá.

Követendőnek tartom az Európai Unióban működő adatvédelmi tisztviselők munkajogi védelmére vonatkozó rezsimet, nevezetesen, hogy a tisztviselő csupán akkor bocsátható el állásából idő előtt, amennyiben azt az adatvédelmi felügyeleti hatóság is jóváhagyja.[235] Ennek minden adatvédelmi tisztviselőre való kiterjesztése elősegítené a független működést. Láttuk, a független működés fontos garanciája annak, hogy az adatvédelem, privacyvédelem szempontjai minden külső nyomás nélkül jelenhessenek meg a döntéshozatal során. Ez a pótlólagos védelem kiegészíthető a határozott idejű kinevezéssel, amely elejét veheti egy rosszul működő munkahelyi közeg határozatlan idejű fenntartásának.

[235] Az Európai Parlament és a Tanács (EU) 2018/1725 rendelete (2018. október 23.) a természetes személyeknek a személyes adatok uniós intézmények, szervek, hivatalok és ügynökségek általi kezelése tekintetében való védelméről és az ilyen adatok szabad áramlásáról, valamint a 45/2001/EK rendelet és az 1247/2002/EK határozat hatályon kívül helyezéséről 44. cikk (8) bekezdése szerint: „[a]z adatvédelmi tisztviselőt az őt kijelölő uniós intézmény vagy szerv mentheti fel, ha az adatvédelmi tisztviselő már nem felel meg a feladatának teljesítéséhez előírt feltételeknek, és csak az európai adatvédelmi biztos hozzájárulásával".

Említettem, hogy Hustinx az első vonalban feladatot ellátó személyekként tekint a tisztviselőkre. Ez az információs előnyük tovább erősítendő, és állítandó a magánszféra védelmének szolgálatában. Javaslatom szerint, amennyiben a tisztviselőt foglalkoztató adatkezelő szervezet új adatkezelést kíván bevezetni, és ezt a tisztviselő ellenzi, úgy azt be kell jelenteni az adatvédelmi hatóságnak. Ahogyan azt Simon Éva már 2008-ban[236] javasolta, az adatvédelmi hatásvizsgálat intézményét ki kell terjeszteni, ennek hasznos hatásai mind a közszférában, mint pedig a magánszférában jelentkeznének.

Simon Éva azzal érvelt, hogy nem csupán adatvédelmi szempontokat, hanem kifejezetten üzleti szempontokat is szolgál az új intézmény bevezetése. A közszférára és a magánszférára vonatkozóan hat pontban foglalta össze javaslatait: „1. Kötelezővé kell tenni az adatvédelmi hatásvizsgálatok elvégzését valamennyi állami szervnél, ahol olyan intézkedést terveznek, amely személyes adatok kezelését érinti, illetve ha az intézkedés az adatvédelmi szabályozás módosításával jár;
2. Kötelezővé kell tenni az adatvédelmi hatásvizsgálatok elvégzését azoknál az adatkezelőknél, ahol belső adatvédelmi felelős kinevezése kötelező, ha az adatkezelést érintő lényeges intézkedést terveznek;
3. Garanciális elemként érdemes bevezetni a független szervezetek által készített vizsgálati eredményt, amelyet az adatvédelmi biztosnak kötelező lenne megküldeni;
4. A hatásvizsgálatokat nyilvánosságra kell hozni mind az azt végző szervezetnek, mind a kormányzati/közigazgatási szerveknek;
5. A nyilvánosságra hozott hatásvizsgálat eredményét az érdekelt társadalmi szervezetek és érdekképviseleti szervek véleményezhessék;
6. Szükséges kidolgozni az adatvédelmi hatásvizsgálat követelményrendszerét és annak figyelembevételére vonatkozó kötelezettséget, mulasztása esetén annak szankcióját.”

Bár az általam javasolt modell nem az adatvédelmi hatásvizsgálatra épül, hanem alapvetően arra, hogy az adatvédelmi tisztviselő nyilvánítson véleményt a tervezett adatkezelés jogszerűségéről, Simon javaslata egybecseng az általam felvázoltakkal.

[236] Simon Éva: Az adatvédelmi hatásvizsgálat bevezetésének lehetősége. In Székely Iván – Szabó Máté Dániel (szerk.): *Szabad adatok, védett adatok*. Budapest, Információs Társadalomért Alapítvány, 2008. 212.

Az előzőeknek megfelelően e helyütt nem kívánok arról értekezni, hogy az adatvédelmi tisztviselő milyen módszertan szerint alakítja ki álláspontját a javasolt új intézkedéssel kapcsolatban. Az adatvédelmi hatásvizsgálat által nyújtott transzparenciakötelezettség valóban korlátos. Azt a 29. cikk szerinti munkacsoport is elismerte, hogy a rendelet nem követeli meg a hatásvizsgálat nyilvánosságra hozatalát, ugyanakkor a munkacsoport szerint érdemes azt „mérlegelni", hiszen „ezáltal növelhető az adatkezelő adatkezelési műveletei iránti bizalom". Különösen hasznos a nyilvánosságra hozatal, ha az adatkezelési művelet „a nyilvánosságot érinti", illetve ha „közhatalmi szerv végez hatásvizsgálatot". Az természetes, hogy nyilvánosságra hozatal esetén a biztonsági kockázatokról, üzleti titkokat vagy bizalmas üzleti információkat felfedő információkról nem kell tájékoztatást nyújtani.[237] Mindazonáltal fontos garanciát jelentene, ha a jogi megfelelés belső ellenőrzés útján, a tulajdonosi érdekektől független módon elvégezhető lenne. Olyan mélységű ellenőrzést jelentene ez, amelyre az adatvédelmi hatóságok a jelenlegi modell szerint képtelenek lennének. Buzás Péter, bár nem fejti ki ezt bővebben, az adatvédelmi tisztviselőket egyfajta belső „ellenőrző hatóságként" azonosítja. Az általam leírt szabályozási keretben helyeselni tudom a szakirodalomban megjelent, Buzás által is említett irányt.[238]

Sulyok Tamás az ügyvédi hivatás alapjogvédelmi funkcióját is hangsúlyozza, továbbá azt is, hogy az ügyvédi függetlenség a tisztességes eljáráshoz való jog érvényesülésének biztosítéka.[239] Bár a tisztviselő és az ügyvéd markánsan eltérő szerepet tölt be, a gyakorlat azt igazolja, hogy a két szerep gyakran „összecsúszik", és ügyvédek, ügyvédi irodák látnak el tisztviselői feladatokat. Ami a tisztviselő alapjogvédelmi feladatát illeti, az ügyvédi feladatoktól ez nem idegen, ahogyan Sulyok is utal erre. Mindazonáltal nem tagadható, hogy a tisztviselő esetleges bírságolása – ahogyan arról szintén szólok – a függetlenség terén sajátos helyzetet teremt. Ahogyan az adatkezelőtől való egzisztenciális függőség, úgy a bírság kockázata is

[237] Vö. A 29. cikk alapján létrehozott adatvédelmi munkacsoport iránymutatása az adatvédelmi hatásvizsgálat elvégzéséhez és annak megállapításához, hogy az adatkezelés az (EU) 2016/679 rendelet alkalmazásában „valószínűsíthetően magas kockázattal jár-e", az elfogadás időpontja: 2017. április 4. 21. Forrás: a NAIH honlapja.

[238] Péterfalvi Attila – Révész Balázs – Buzás Péter: *Magyarázat a GDPR-ról*. Budapest, Wolters Kluwer Hungary, 2018. 245.

[239] Sulyok Tamás: *Az ügyvédi hivatás alkotmányjogi helyzete*. Szeged, Pólay Elemér Alapítvány, 2015. 91–91., 155.

jelentősen befolyásolhatja a tisztviselő működését. A cél a megfelelő egyensúly megtalálása, ahol a jogvédelmi optimum elérhető.

Szükséges az új tisztviselői szerep a leírt védelmi deficit ellensúlyozására. Az adatkezelők oldalán fennálló transzparenciahiányt fel kell számolni, és ennek hathatós eszköze lenne a konfliktusbejelentési kötelezettség. A bejelentés önmagában nem járna hatósági ellenőrzési kötelezettséggel a hatóság oldalán, azonban az incidensek bejelentéséhez hasonlóan abban a helyzetben lenne a hatóság, hogy maga mérlegelje, van-e teendője a bejelentett konfliktussal összefüggésben.

Ez az új rezsim jelentős változást eredményezne az adatkezelő és a tisztviselő együttműködésében, azonban nem tartom elkerülhetőnek a tisztviselői pozíció erősítését ezen intézkedések nélkül. A tisztviselő a védelmi deficit ellensúlyozására hivatott, ennek megfelelően pozíciója erőteljes reformra szorul a közeli jövőben. Ennek lehetséges modelljét vázoltam fel az előzőekben.

Vákát

A Rendelet egyes jogintézményeinek részletes elemzése – az adatvédelmi felügyeleti hatóságok

Az Európai Unió 1995-ben elfogadott 95/46/EK számú adatvédelmi irányelve írta elő, hogy „minden tagállamnak rendelkeznie kell arról, hogy az ezen irányelv értelmében a tagállam által elfogadott nemzeti rendelkezéseknek a területén történő alkalmazását valamely hatóság vagy hatóságok felügyeljék".[240] Az 1995-ös elfogadást megelőzően is számos uniós, valamint uniós tagságra készülő államban működött már adatvédelmi felügyeleti szerv valamilyen formában.

Magyarországon az Országgyűlés 1995 nyarán választotta meg az első adatvédelmi biztost. Ennek is szerepe volt abban, hogy 2000-ben Magyarország tekintetében az Európai Unió megállapította, hogy megfelelő védelmi szintet biztosít. Az uniós csatlakozást követően ennek gyakorlati jelentősége már nem volt, mindazonáltal ez 2000-ben jelentős eredmény volt, amit az is aláhúz, hogy egyetlen másik tagjelölt állam sem kapott ilyen minősítést a csatlakozást megelőzően.
Európában az első klasszikus adatvédelmi hatóság Franciaországban jött létre. A Commission Nationale de l'Informatique et Liberté 1978 óta látja el ezt a feladatot.

Az irányelv azt is előírta, hogy a hatóságok a rájuk ruházott feladatok gyakorlása során teljes függetlenségben járnak el. Bár addigra több európai államban hagyományosan működtek adatvédelmi hatóságok, az Európa Tanács 1981-es egyezménye (108-as egyezmény) nem rögzítette kötelező jelleggel létrehozatalukat. Ezt a kötelezettséget majd csak két évtizeddel később a kiegészítő jegyzőkönyv határozta meg 2001-ben. Az irányelv átültetésének határideje 1998 volt, ez az a dátum tehát, amelytől kezdődően az Európai Unió jogában a kötelezően létrehozott, független adatvédelmi felügyeleti szervekről beszélhetünk. Az Európai Unió akkori tagállamai

[240] Az Európai Parlament és a Tanács 95/46/EK irányelve (1995. október 24.) a személyes adatok feldolgozása vonatkozásában az egyének védelméről és az ilyen adatok szabad áramlásáról, 28. cikk.

közül utoljára az Egyesült Királyságban jött létre adatvédelmi hatóság. Az Information Commissioner's Office csak az irányelv átültetési határidejének lejártakor, 1998-ban kezdte meg működését.

A felügyeleti hatóságok szerepe

A szakirodalomban kevés forrás foglalkozik azzal, hogy az adatvédelmi hatóságoknak pontosan mi a szerepe, és szintén kevesen elemzik, hogy mi végre jönnek létre ezek, milyen megfontolások teszik szükségessé a felügyeleti szervek létrehozását. A továbbiakban e kevés forrás feldolgozása révén elemzem az adatvédelmi hatóságok alkotmányos helyét és szerepét.

Mint minden jogi norma, így az adatvédelmi szabályok kikényszerítésének lehetősége is alapvető kérdés a jogszabályok érvényesülésében. Az adatok alanya az érintett három fórum előtt kereshet lehetőséget arra, hogy jogainak érvényt szerezzen: először közvetlenül az adatok kezelőjénél, másodszor az adatvédelmi hatóságnál és végül a bíróság előtt.

A jogok érvényesítésében nincs kényszerű sorrendiség, az érintett maga választhatja meg, hogy mely fórum előtt kívánja kérelmét előterjeszteni. A kényszerű sorrendiség hiánya két ponton megszorítóan értelmezendő: amennyiben az érintett az adatkezelő előtt még nem terjesztett elő a joga érvényesítése érdekében kérelmet, vagy az ennek teljesítésére rendelkezésre álló határidő még nem telt el, az adatvédelmi hatóság a kérelmet idejekorán beterjesztettként el fogja utasítani. Az adatvédelmi hatóság nem járhat el olyan ügyben, amelyben már született bírósági ítélet, vagy bírósági eljárás van folyamatban. Az Infotv. 53. cikk (3) bekezdésében rögzített eljárásjogi szabály azt hivatott szolgálni, hogy egyazon ügy megítélésében ne születhessen a bíróság ítéletével párhuzamosan hatósági döntés is: „[a] Hatóság a bejelentést érdemi vizsgálat nélkül elutasítja, ha az adott ügyben bírósági eljárás van folyamatban, vagy az ügyben korábban jogerős bírósági határozat született".

A jogszabályokban nevesített jogok bíróság előtti érvényesítésénél lényegesen rugalmasabb, olcsóbb és gyorsabb lehetőséget kínál a hatósági kikényszerítés. Sőt, önmagában a felügyeleti szerv létrehozatala jelentős hatást gyakorol a jogok érvényesülésére.

Hustinx is azzal érvel, hogy szükséges volt a hatóságok létrehozása, mert ha csupán bírósági jogorvoslat állt volna az érintett rendelkezésére, akkor

ez hátrányos helyzetbe sodorta volna az adott esetben kevés információval rendelkező érintettet, és teljességgel az ő kezdeményezésére bízta volna a szabályozás a jogorvoslat lehetőségét. Emellett Hustinx szerint hatóságok hiányában hosszú időbe telt volna, mire az adatvédelmi rendelkezéseknek preventív szerepe lett volna, nem beszélve arról, hogy a jogalkalmazás során az egységes megközelítés kárt szenvedett volna.[241]

Nem csupán szimbolikus jelentősége van annak, ha egy állam adatvédelmi felügyeleti szervet hoz létre,[242] hanem olyan intézményi keretet is teremt ezáltal, amely a védelem megteremtésének és későbbi erősítésének elengedhetetlen része.

Az Európai Unió jogában is megfigyelhető ez a tendencia. Először csupán a tagállamok önkéntes döntésétől függően jöttek létre adatvédelmi felügyeleti szervek az 1995 előtti időszakban. Második lépésben az Európai Unió adatvédelmi irányelve kötelezően előírta ilyen szervek létrehozását. Ennél a fázisnál meg kell jegyeznünk, hogy az irányelv a feladat- és hatáskörre nézve nem adott pontos iránymutatást, ezért a tagállami szervek feladat- és hatásköre nem volt egységes. Például nem mindegyik szabhatott ki adatvédelmi bírságot, ez pedig sok más körülmény mellett a védelmi szintek közötti különbségekhez vezetett. Az adatvédelmi felügyeleti szervek hatáskörei között már a nyolcvanas években is jelentős különbségek voltak. Simitis 1987-ben publikált írásában azt állapította meg, hogy míg Norvégiában vagy Ausztriában beavatkozási jogot kaptak az adatvédelmi hatóságok, addig a nyugatnémet jog a nyilvános viták erejében hitt, és ennek megfelelően a parlamenti biztos a tapasztalt jogsértésre csupán a figyelmet tudta felhívni – a parlamenten belül, illetve a szélesebb közvélemény előtt. Ebben azonban ki is merültek a lehetőségei.[243]

Végül pedig a Rendelet előírta a hatósági jogkörrel felruházott adatvédelmi felügyeleti hatóságok létrehozását, azonos feladat- és hatáskörrel. Ez a tendencia tehát a védelem erősítésének irányába mutat, amelynek első fázisa azért különösen jelentős, mert a védelem kiterjesztésének alapját teremti meg.

[241] Hustinx (2009): i. m. 134.

[242] Az Európai Unió Bírósága az adatvédelmi hatóságokat az adatvédelem őreinek *(guardians of data protection)* tekinti, C-518/07-es számú ügy, Bizottság versus Németország, EU:C:2010:125, 23.

[243] Spiros Simitis: Reviewing Privacy in an Information Society. *University of Pennsylvania Law Review,* 135. (1987), 3. 745.

A Rendeletben a jogalkotó is úgy fogalmaz, hogy a fennálló védelem alapvető alkotóeleme, hogy a tagállamokban teljes függetlenséget élvező felügyeleti hatóságokat hozzanak létre.[244] Amint azt a későbbiekben bemutatom, a védelem szintjének erősítésében jelentős szerepe van annak, hogy a felügyeleti hatóság milyen módon látja el feladatait, illetve gyakorolja hatásköreit.

Az adatvédelmi hatóságok létrehozásának szükségességéről

Az adatvédelmi felügyeleti szerveknek szánt szerepet kiemeli az Európai Unió működéséről szóló szerződés 16. cikke, amely a független adatvédelmi hatóságokról rendelkezik. Az EU jogában az adatvédelmi hatóságok ilyen módon alkotmányos státuszt[245] nyernek. Hielke Hijmans szerint a tagállami adatvédelmi hatóságok ezáltal nem válnak az EU intézményeivé, mindenesetre a Rendelet egységesítő-harmonizáló céljával összhangban létüket és mandátumukat a tagállami jogalkotótól függetleníti. Az adatvédelmi hatóságok az EU jogának is érvényt kell hogy szerezzenek, ilyen módon az uniós adminisztráció részének tekinthetjük őket, miközben a tagállamok szintjén jönnek létre és működnek.

Simitis a hatékony jogvédelem elengedhetetlen eszközének tekinti, hogy a személyes adatokat csupán meghatározott célból lehessen felhasználni. Az adatok felhasználására szolgáló technológia folyamatosan változik (Simitis írása 1987-ben született), ezért a jogszabályokat folyamatosan felül kell vizsgálni a változó technológia és az adatok szisztematikus felhasználásának fényében. Amennyiben a jogalkotó meg szeretné őrizni a kontrollt az adatkezelések fölött, akkor a szabályok folyamatos felülvizsgálata mellett kell elköteleznie magát.[246]

Az adatvédelmi felügyeleti hatóságot szintén a védelem alapjai között határozza meg.[247] Úgy ítéli meg, hogy nem elegendő az adatvédelmi szabá-

[244] A Rendelet (117) preambulumbekezdésének első mondata szerint.

[245] Hijmans disszertációjában az adatvédelmi hatóságok általános felépítését a következőképpen nevezi meg: alkotmányos státusszal rendelkező szakértő szervek, amelyeknek az információs társadalomban szerepük van. Hijmans (2016): i. m. 287–288.

[246] Simitis (1987): i. m. 741–742.

[247] Simitis (1987): i. m. 742.

lyok megalkotása, azok figyelemmel kíséréséről is gondoskodni kell. Sem az érintettek kontrollja, sem a hagyományos jogorvoslati utak nem elégségesek. Az adatkezelő szervezetén belül folyamatos konfliktushoz vezetne a kontroll, ezért egy külső szereplőre kell azt bízni. Ez a szerv pedig egy független adatellenőrző hatóság *(Independent Data Control Authority).* Simitis az érintett helyzetét illetően ma is időszerű kételyt fogalmaz meg: még ha az érintett számára kontroll-lehetőséget biztosítana is a jog, az állami és magánszervezetek adatkezeléseit kívülállóként nem tudná megítélni, hiszen az ehhez való információktól meg van fosztva. Az általam említett védelmi deficitre mutat rá itt Simitis is. A 21. században is ugyanezzel a problémával küzd az érintett és az adatvédelmi hatóság is: nincsen hiteles forrásból származó ismerete az adatok kezeléséről, ennek megfelelően hatékony beavatkozási lehetőség nélkül a védelem szükségszerűen alacsony szinten áll.[248]

Az Európa Tanács úgynevezett 108-as egyezményének kiegészítő jegyzőkönyvéhez fűzött magyarázat szerint az Egyezményben foglalt elvek alkalmazásának javítása áll a független adatvédelmi hatóságok létrehozatala mögött. Az adatvédelmi felügyeleti hatóságok a védelmi rendszer lényeges elemévé váltak a demokratikus társadalmakban.[249] Hustinx is a hatóságok létrehozatala mellett érvel, de három feltételt is megjelöl: a hatóságok hatékonyan láthassák el feladataikat, legyen lehetőségük stratégiai megközelítést alkalmazni, továbbá tényleges eredményt legyenek képesek elérni. Hustinx szerint ennek egyik feltétele, hogy a hatóságok saját maguk határozhassák meg prioritásaikat, és ne eméssze fel minden energiájukat az egyes panaszügyek intézése.[250]

Hijmans hat érvet sorol fel az adatvédelmi hatóságok létrehozása érdekében. Elsőként egy történelmi igényt azonosít a kialakult adatvédelmi gyakorlat harmonizálása érdekében. Másodszor az érintettek számára nyújtandó hatékony védelmet említi. Harmadik helyen azt a sajátosságot hozza fel, ami minden adatvédelmi kérdés kapcsán felmerül: szakértelmet igényel az adatkezelési műveletek vizsgálata, ami egy szakértői szerv

[248] Simitis (1987): i. m. 742–743.

[249] *Explanatory Report to the Additional Protocol to the Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data, Regarding Supervisory Authorities and Transborder Data Flows.* Strasbourg, 2001. november 8.

[250] Hustinx (2009): i. m. 131–135.

létrehozásának irányába mutat. Negyedik helyen a piaci szereplők és a kormányzati szervek felügyeletének szükségességét említi. E felügyeleti szerep teszi nélkülözhetetlenné, hogy a felügyeleti hatóságok teljes függetlenségben láthassák el feladataikat. Akár a piaci, akár a kormányzati szereplőktől való függés összeegyeztethetetlen a felügyeleti szereppel. A politikailag független intézmény iránti igényt említi ötödik helyen, végül hatodikként az intézményi letisztultság mellett érvel, nevezetesen előnynek tekinti, ha egy szervezet csupán egytípusú feladattal foglalkozik.

Bennett és Raab az adatvédelmi hatóságok funkciói között azonosítják az ombudsmani, az ellenőri, a konzultációs, az oktatási, a politikai tanácsadói, az engedélyezési és a kikényszerítési szerepet.[251] E hét szerep között lehetnek hangsúlyeltolódások, de a nemzetközi gyakorlat alapján ezek teszik az adatvédelmi hatóságokat azzá, ami a szerepüket megkülönbözteti minden más szereplőtől.

A magam részéről általánosságban osztom Hijmans megközelítését, mindazonáltal vitatom, hogy egy szervezet csupán egy területre összpontosíthat hatékonyan. Szerte a világban működnek hatékonyan adatvédelmi hatóságok, amelyeknek az információszabadság területén is van hatáskörük.[252] A teljes profiltisztítást nem tartom nélkülözhetetlennek az adatvédelmi hatóságok esetében. A politikai függetlenség mellett azt is fontosnak tartom, hogy a szabályozó szerep és a felügyeleti szerep között ne alakuljon ki konfliktus. Az adatvédelmi hatóságok a Rendelet szerint számos ponton alakítják az adatkezelések gyakorlatát, fontos ügyelni arra, hogy a két szerep, a szabályozó és a felügyeleti szerep ne vezessen ahhoz, hogy a hatóság végül saját álláspontját kénytelen megvizsgálni vagy nem kívánatos esetben akár felülvizsgálni egy konkrét eljárás során.[253]

[251] Colin J. Bennett – Charles D. Raab: *The Governance of Privacy – Policy Instruments in Global Perspective*. London, The MIT Press, 2006. 133–143.

[252] Az International Conference of Information Commissioners (ICIC) tagnyilvántartása szerint Európában ilyen vegyes modellt követ Albánia, az Egyesült Királyság, Észtország, Franciaország, Magyarország, Málta, Montenegró, Németország szövetségi szinten, de például Berlinben is, Svájc és Szerbia. A modell Európán kívül is népszerű, így például Kanadában, Ausztráliában, de Ázsiában is működik. Forrás: az ICIC honlapja.

[253] Vö. Jóri András: Shaping vs Applying Data Protection Law: Two Core Functions of Data Protection Authorities. *International Data Privacy Law,* 5. (2015), 2. 133–143.

Az adatvédelmi felügyeleti hatóságok létrehozatala a védelmi lépcső elméletének fényében

Az előzőekben elemeztem azokat az érveket, amelyek a felügyeleti hatóságok létrehozatalát alátámasztják. Ezek részben elméleti, részben kifejezetten gyakorlatias megfontolások. A szakirodalomban nincsen vita arról, hogy az adatvédelem jogának kikényszerítésére a megfelelő intézményi forma az önálló és független hatóság. Természetesen adódik az üzleti szereplőktől és a kormányoktól független működés követelménye.

A hatóságok létrehozását az abszolút kiindulópontnak, a vitathatatlan egyes szintnek tekintem a védelmi lépcsőn. Ezek létrehozatala előtt az adatvédelmi jog gyakorlatilag mindazon követelmények híján van, amelyeket az imént a hatóságok létrehozatala mellett felsorakoztattam. Ezen érvek sora pedig jelentős akkor, amikor azt kell megállapítanunk, hogy a független és professzionális felügyeleti szerv nélküli szabályozás lényegesen alacsonyabb védelmi szintet ígér, mint annak létrehozását követően.

A felügyeleti hatóság létét illetően csak két fokot azonosíthatunk a védelmi lépcsőn, ez pedig a létrehozatalt megelőző és a létrehozatalt követő. Azért is jelentős lépés az intézmény megalkotása, mert a létező intézmény megszüntetése olyan markáns változás lenne, amely nem támasztható alá a védelmet erősítő érvekkel. A hatóságok feladatait és hatáskörét az alábbiakban fogom vizsgálni. Már előzetesen megállapítható, hogy a független hatóságok léte nélkül nincs értelme védelemről beszélni, illetve a védelem szintjéről értekezni.

A hatóságok statikus pontot jelentenek a védelem rendszerében, mozdíthatatlan intézményt, amelyre a védelem sok eleme épül, illetve amelytől a védelem szintje sok tekintetben függ.

A hatóságok feladatai – a védelem erősítésének és egységesítésének eszközei

A Rendelet a hatóságokat minden tagállamban ugyanazokkal a feladatokkal és tényleges hatáskörökkel ruházza fel.[254] Az egységesítés a jogalkotó egyértelmű szándéka, amellyel azonos védelmi szintet kíván teremteni az egész Európai Unióban. A védelmi szint egységesítése pedig a jogvédelmen túl

[254] A (129) preambulumbekezdés első mondata szerint.

az adatok szabad áramlásának előfeltétele is. A tagállamok ugyanis nem korlátozhatják az adatok szabad áramlását arra hivatkozással, hogy a másik tagállamban nem kielégítő az adatvédelem szintje.

Ez az elvárás az 1995-ös irányelvben is megjelent már. Az 1. cikk (2) bekezdése szerint a „tagállamok nem korlátozhatják és nem tilthatják a személyes adatok tagállamok közötti szabad áramlását az (1) bekezdés értelmében biztosított védelemmel kapcsolatos indokok miatt". A Rendelet 1. cikk (3) bekezdése gyakorlatilag azonos szabályt tartalmaz: „A személyes adatok Unión belüli szabad áramlása nem korlátozható vagy tiltható meg a természetes személyeknek a személyes adatok kezelése tekintetében történő védelmével összefüggő okokból."

Az alábbiakban a hatóságok feladatait csoportosítom, és e szempontok szerint mutatom be az egyes feladatokat.

Általános feladatok

A Rendelet huszonkét pontban határozza meg a hatóságok feladatait. Általános feladatként értékelhető az első pont, amely szerint a hatóság nyomon követi és kikényszeríti a Rendelet alkalmazását. Ennek keretében vizsgálatot folytat a Rendelet alkalmazásával kapcsolatban.

A Rendelet 57. cikk (1) bekezdés a) és h) pontjának megfelelően a nyomon követés legkézenfekvőbb módja, hogy a nyilvánosan elérhető információk, sajtóhírek alapján a hatóságok figyelemmel kísérik az adatkezelők és az érintettek helyzetét befolyásoló körülményeket. A sajtófigyelés és a személyes adatok védelmével összefüggő jogszabálytervezetek rendszeres nyomon követése például a magyar adatvédelmi hatóság mindennapos feladatai közé tartozik.

A köz és az érintettek irányába mutató feladatok

A feladatok egy része általában a köz irányába mutat, így a hatóságok elősegítik a nyilvánosság figyelmének felkeltését és az ismeretek terjesztését,

ennek során különös figyelmet fordítanak a gyermekekre.[255] A feladatok egy másik része kifejezetten az érintettekre irányul: a felügyeleti hatóság tájékoztatást ad az érintettnek a Rendelet alapján őt megillető jogok gyakorlásával kapcsolatban, továbbá kivizsgálja az érintett által benyújtott panaszokat. Az érintetti panaszok benyújtását a hatóság köteles megkönnyíteni, például elektronikus úton kitölthető formanyomtatvány létrehozásával. Ezt a feladatát látja el a hatóság akkor is, amikor az érintettek számára a joggyakorlást megkönnyítő ismertetőket tesz közzé.[256]

A hatóságok belső feladatai

A feladatok egy újabb csoportja belső tevékenységre irányul, a hatóságok kötelező feladatai közé tartoznak, hogy figyelemmel kísérjék az adatok védelmére kiható fejleményeket, különösen az információs és kommunikációs technológiák, valamint a kereskedelmi gyakorlatok fejlődését. A belső feladatok közé tartozik még az, hogy a hatóság nyilvántartást vezet a Rendelet megsértéséről és a meghozott intézkedésekről. A hatóságok e téren figyelemmel kísérik a publikált tudományos eredményeket, és a nemzetközi gyakorlat része, hogy technológiai hátterű jogkérdéseket a tudományos élet képviselőivel konferenciák, különböző együttműködések keretében vitatnak meg.[257]

A jogalkotási és közigazgatási tervezetek véleményezése

Külön nevesített feladata a felügyeleti hatóságnak, hogy tanácsot ad a jogalkotónak az érintettek védelmét érintő jogalkotási és közigazgatási intézkedések kapcsán. A NAIH a honlapján valamennyi olyan állásfoglalást

[255] A Rendelet 57. cikk (1) bekezdés b) pontja. Kifejezetten a gyermekek védelmét szolgálta az a vizsgálatsorozat, amelynek során a NAIH a gyermekek számára is elérhető társkereső oldalak adatkezeléseit vizsgálta próbaregisztrációk keretében. Ilyen vizsgálatokat folytatott a hatóság a NAIH-5951/2012/H, a NAIH-798/2013/, a NAIH-799/203/H, a NAIH-800/2013/H, a NAIH-801/2013/H, a NAIH-802/2013/H, a NAIH-803/2013/H, a NAIH-805/2013/H, valamint a NAIH/2015/187/H számú ügyekben.

[256] A Rendelet 57. cikk (1) bekezdés e) és f) pontja.

[257] A Rendelet 57. cikk (1) bekezdés i) és u) pontja.

közzétesz, amely jogszabályok véleményezése körében született.[258] Az előzetes véleményezési lehetőség a védelem megőrzésének fontos garanciája, hiszen az életviszonyok szabályozása terén ilyen módon megelőzhetők a védelmet adott esetben hátrányosan érintő intézkedések. Ez a feladat akkor teljesíthető felelősségteljesen, ha a véleményezésre elegendő idő áll rendelkezésre, továbbá a jogalkotó a magánszférára gyakorolt hatások tekintetében a hatásvizsgálatot elvégezte.

Kötelező adatkezelés esetén az adatvédelmi hatásvizsgálatot az adatkezelést előíró jogszabály előkészítője folytatja le az Infotv. 25/G. § (6) bekezdése szerint. Az adatvédelmi hatásvizsgálat tartalmazza legalább a tervezett adatkezelési műveletek általános leírását, az érintettek alapvető jogainak érvényesülését fenyegető, az adatkezelő által azonosított kockázatok leírását és jellegét, az e kockázatok kezelése céljából tervezett, valamint a személyes adatokhoz fűződő jog érvényesülésének biztosítására irányuló, az adatkezelő által alkalmazott intézkedéseket.

Együttműködés más felügyeleti hatóságokkal és az Európai Adatvédelmi Testület munkájában való részvétel

A Rendelet egyik legfontosabb újításának megfelelően szorosan együttműködik más felügyeleti hatóságokkal, amelynek célja a Rendelet egységes alkalmazásának és érvényesítésének biztosítása. Ezen túl pedig az Európai Adatvédelmi Testület tevékenységéhez hozzájárul.[259] Ez utóbbi azt is jelenti, hogy a NAIH Magyarországot képviseli a testületen belül. A felügyeleti hatóságok közötti együttműködésről lejjebb bővebben is szólok.

Az adatkezelőkkel és adatfeldolgozókkal összefüggő feladatok

A feladatok legnagyobb része kifejezetten az adatkezelőkre, illetve adatfeldolgozókra irányul, valamint az ő tevékenységükkel függ össze. Ezek körében a hatóság felhívja az adatkezelők figyelmét a Rendelet szerinti

[258] A Rendelet 57. cikk (1) bekezdés c) pontja.
[259] A Rendelet 57. cikk (1) bekezdés g) és t) pontja.

kötelezettségeikre;[260] jegyzéket állít össze az adatvédelmi hatásvizsgálatra vonatkozóan;[261] tanácsot ad az adatkezelő számára az adatvédelmi hatásvizsgálat alá eső adatkezelési műveletekkel kapcsolatban;[262] ösztönzi a magatartási kódexek létrehozását, illetve jóváhagyja azokat; ösztönzi tanúsítási mechanizmusok létrehozását, illetve jóváhagyja a tanúsítási szempontokat; ez utóbbiak körében közzéteszi az ellenőrző, illetve tanúsítószervezet akkreditációjára vonatkozó szempontokat, és elvégzi e szervezetek akkreditációját.[263]

A külföldre irányuló adattovábbítással összefüggő feladatok

A külföldre való adattovábbítást illetően a felügyeleti hatóság bizonyos szerződési feltételekről, illetve egyéb garanciákról dönt. Engedélyez szerződéses feltételeket és rendelkezéseket, jóváhagyja a kötelező erejű vállalati szabályokat.[264]

További, tagállami szinten meghatározott feladatok

A feladatok felsorolása azzal zárul, hogy a hatóság a személyes adatok védelméhez kapcsolódó minden más feladatot ellát.[265] A tagállami jogalkotó a felügyeleti hatóság számára további feladatokat állapíthat meg. Ennek uniós jogi korlátja, hogy a további feladatok nem veszélyeztethetik

[260] Az adatvédelmi tisztviselők kinevezésével kapcsolatban a NAIH például a Rendeletre való felkészülés lázas időszakában közleményben arra hívta fel a figyelmet, hogy a Rendelet által előírt felkészültség néhány napos képzés keretében nem szerezhető meg, még akkor sem nyújt semmiféle garanciát, ha állami regisztrációra hivatkozással ígérik ezt. Forrás: a NAIH honlapja.

[261] A Rendelet 35. cikk (4) bekezdése szerinti feladatának megfelelően a NAIH is nyilvánosságra hozta azon adatkezelések listáját, amelyek esetében a hatásvizsgálat kötelezően végzendő el. Forrás: a NAIH honlapja.

[262] Ha a hatásvizsgálat arra az eredményre vezet, hogy a kockázat mérséklésére tett intézkedések ellenére is valószínűsíthetően magas kockázat áll fenn, az adatkezelés megkezdése előtt az adatkezelőnek konzultálnia kell a felügyeleti hatósággal – a hatóságnak pedig az adatkezelő rendelkezésére kell állnia. A részletes szabályokat a Rendelet 36. cikke rögzíti.

[263] A Rendelet 57. cikk (1) bekezdés d), k), l), m), n), o), p) és q) pontja.

[264] A Rendelet 57. cikk (1) bekezdés j), r) és s) pontja.

[265] A Rendelet 57. cikk (1) bekezdés v) pont.

a Rendelet hatékony érvényesülését, egyébként a tagállami jogalkotó szabadon határozhatja meg a hatóság további teendőit. A magyar felügyeleti hatóságot, a NAIH-ot a magyar szabályozás hagyományainak megfelelően adatvédelmi feladatai mellett a jogalkotó az információszabadság és a titokfelügyelet terén is felruházta feladatokkal és hatáskörökkel. Ez utóbbiak értelemszerűen nem élvezhetnek prioritást a személyes adatok védelmével összefüggő feladatok kárára, ezért a jogalkotó, illetve a NAIH költségvetését jóváhagyó Országgyűlés felelőssége, hogy ezek ellátása a Rendelet végrehajtását ne hátráltassa.

Ingyenesség

A felügyeleti hatóság úgy látja el feladatait, hogy azok az érintett, illetve adott esetben az adatvédelmi tisztviselő számára térítésmentesek legyenek.[266] Az adatalanyok esetében a jogorvoslathoz való hozzáférés ingyenessége természetes jogállami elvárás *(access to justice),* hogy vitás ügyeikben, jogaik védelme érdekében könnyen és hatékonyan lépjenek fel.[267] Ez az előírás szolgálja egyrészt az adatalanyok joggyakorlásának megkönnyítését, másrészt pedig az adatvédelmi tisztviselők munkájának támogatását. Az ingyenesség mind a két szereplő esetében hozzájárul a védelem szintjének erősítéséhez. A Rendelet által megalkotott rendszer fontos szereplői az adatvédelmi tisztviselők, akik jelentősen járulhatnak hozzá az érintetti jogok adatkezelői szervezeten belüli érvényesítéséhez, az adatkezelő szervezeten belül az adatvédelmi kultúra kialakításához.

[266] Az ingyenességet az 57. cikk (3) bekezdése írja elő.

[267] Az *access to justice* témájára az adatvédelem terén viszonylag ritkán hivatkoznak. A panasztétel joga kapcsán is szólok arról, hogy ez egy könnyen elérhető, ingyenes jogorvoslat. A témáról bővebben szól a Fundamental Rights Agency kiadványa: *Handbook on European Law Relating to Access to Justice.* European Union Agency for Fundamental Rights and Council of Europe, 2016.

A felügyeleti hatóságok feladatai a védelmi lépcső és a jog hatékonyságának fényében

Az adatvédelmi felügyeleti hatóságok feladatai a Rendelet révén egységesedtek. Az adatvédelmi irányelv a teljes egységesítést nem várta el a tagállamoktól, ez az uniós jogalkotási aktus típusából adódik. Feltehetően az irányelvet megelőző jogalkotási folyamatban az irányelvi szabályozásnál pontosabb követelmények meghatározása nem élvezett konszenzust, a köztes megoldás kompromisszumnak tekinthető.

Egységes feladatkör

Kérdés, hogy önmagában a feladatok egységesítése előrelépésnek tekinthető-e a védelmi lépcsőn. A védelmi lépcső elméletéből kiindulva minőségi előrelépésre van szükség ahhoz, hogy a rendeleti szabályokat a Rendeletet megelőző időszakkal összevetve egy magasabb fokként határozhassuk meg. Az egységesítés eredménye az, hogy a tagállami adatvédelmi hatóságok azonos feladataiknak megfelelően alakítják belső szervezetüket, és ilyen háttérrel látják el a saját tagállamukon belül feladataikat, illetve vesznek részt az EGT-n belüli együttműködésben. Ez a közelítés önmagában is elősegíti a hatóságok közötti együttműködést, hiszen a hasonló felépítésű szervezetek szükségszerűen könnyebben és olajozottabban működnek együtt egymással. Ez pedig az érintetti joggyakorlás körében, továbbá az erőforrások hatékonyságában megmutatkozó előnyhöz, védelmi többlethez vezet.

A feladatok bővülésének mennyiségi és minőségi kérdései

A másik kérdés, hogy a feladatok bővülése megvalósul-e, van-e olyan „mennyiségi" előrelépés, amely – mint ahogy arra korábban utaltam – önmagában is előrelépésként értékelendő. Előre kell bocsátani, hogy itt nem az irányelvet átültető tagállami szabályozás, valamint a Rendelet szabályainak összehasonlítását végzem el, hanem ugyanannak a jogalkotónak, az uniós jogalkotó intézményeknek a jogalkotási aktusait elemezzük. Ez az összehasonlítás pedig markáns különbséghez vezet. Az adatvédelmi irányelv a jogszabályok véleményezése, a kérelmek (panaszok) elbírálása, a rendszeres

beszámolási kötelezettség, valamint általában az együttműködés szabályait határozza meg.[268]

A feladatok listája jelentős bővülésen ment keresztül, és ez az adatvédelmi jog fejlődésének jelenlegi fázisában előrelépésként értékelendő. Semmi nem utal ugyanis arra, hogy a felügyeleti hatóságok elértek volna ahhoz a feladatkatalógushoz, amely már minden tekintetben, minden feladatra kiterjedően kielégítő. Ennek alapján arra jutunk, hogy a feladatok számbeli bővülése az erősödő védelem szintjét jeleníti meg. A következő fokozatba való átlépéskor kell majd ismételten mérlegelni, hogy mely feladatok ellátása nem szükséges, vagy éppen hangsúlyosabbá teendő. Ez a mérlegelés előre nem kizárható módon hangsúlyeltolódásokhoz vezethet majd. Ezt egy természetes folyamatnak tekintem, arra is figyelemmel, hogy a hatóságok feladatait magas számban határozta meg a jogalkotó.

A tárgyalt mennyiségi kérdések vezetnek bennünket a hatékonyság tárgyalásának irányába. Annak megállapítása mellett, hogy a Rendelet magasabb szinten képes garantálni a magánszféra védelmét, mint az irányelv idején, és ebben a hatóságok erősödése is szerepet játszik, adódik a kérdés, hogy a feladatokat lehetne-e hatékonyabban ellátni. Akkor, amikor ezt a kérdés megfogalmazódik, nem csupán arra utalhatunk, hogy van a rendeleti szabályozásnál magasabb fok a védelmi lépcsőn. Erre a kérdésre mindig igennel kell válaszolnunk. A válasz akkor is igen kell hogy legyen, ha a következő fok megállapításához még időre, a technológia és az új üzleti modellek magánszférára gyakorolt hatásának jobb megismerésére van szükség.[269] A feltételezés mindenesetre fennáll, hogy vizsgálható és vizsgálandó is, vajon a felügyeleti hatóságok milyen hatékonysággal élnek a magánszféra védelmében a feladataikkal. A Rendelet alkalmazandóvá válása óta e tekintetben a viszonylag kevés eltelt időre is tekintettel nem várhatunk mélyreható elemzést.

A Rendelet értékeléséről és felülvizsgálatáról az Európai Bizottság 2020. május 25-ig, és azt követően négyévente jelentést készít. A jelentést az Európai Parlament és a Tanács elé kell terjeszteni, amelynek elkészítése során a Bizottság az EGT-tagállamokat és azok adatvédelmi hatóságait is bevonja, véleményüket figyelembe veszi.[270] E jelentés előkészítésének

[268] A feladatkört a 95/46/EK adatvédelmi irányelv 28. cikke határozta meg.
[269] Vö. ebben a tekintetben: Szabó (2018): i. m. 35.
[270] Ezt a kötelezettséget a Rendelet 97. cikke írja elő.

keretében, a testület nyilvánosságra hozott álláspontja[271] szerint, a Rendelet eddigi alkalmazása általában sikernek tekinthető. A részleteket illetően azonban kritikát is megfogalmaz, és nem elsősorban az uniós jogalkotóval, hanem saját tagállami kormányzataikkal szemben. A bizottsági álláspont szerint a felügyeleti hatóságok feladat- és hatáskörgyakorlásának hatékonysága nagyban függ a rendelkezésre álló erőforrásoktól. A legtöbb tagállami hatóság pedig úgy nyilatkozott, hogy az elérhető források elégtelenek.[272] Ennek alapján azt kell feltételezni, hogy a tagállami hatóságok jogalkotás nélkül is, pusztán elegendő forrás rendelkezésre bocsátása mellett hatékonyabban tudnák feladataikat ellátni. A költségvetésről rendelkező tagállami döntéshozók ilyen értelemben vett kedvező döntése önmagában is előrelépést jelentene a védelemben. Ennek hiánya pedig alkalmas arra, hogy az uniós jogalkotói célt érdemben hátráltassák.[273]

A 29. cikk szerinti munkacsoport ebben a tekintetben már a Rendelet megalkotásának korai szakaszában konkrét javaslatokat is megfogalmazott, nevezetesen azt, hogy a hatóságok fix feladataihoz egy meghatározott összeget kellene rendelni minden tagállamban, amelyet ki kellene egészíteni azzal a szabállyal, hogy figyelembe veszik a tagállam népességét és a tagállam területén letelepedett multinacionális szervezeteket. Ez a számítási mód sajnos nem vált a gyakorlat részévé.

Az Európai Bizottságnak a Rendelet kétéves alkalmazásának értékeléséről szóló közleménye szerint az eltelt két év nem adott megfelelő időt a részletes értékelésre, de néhány kritikus pontot megemlít, amelyek között a hatóságok szűkös forrásai szintén szerepelnek.[274]

[271] A testület 2020. február 18-i ülésén fogadta el a *Contribution to the Evaluation of the GDPR under Article 97* című állásfoglalását. Forrás: az Európai Adatvédelmi Testület (EDPB) honlapja. *Edpb.europa.eu*.

[272] Testületi állásfoglalás a GDPR értékeléséről, 2–3.

[273] A 29. cikk szerinti adatvédelmi munkacsoport: *2012/1. számú vélemény az adatvédelmi reformjavaslatokról, WP 191,* elfogadás időpontja: 2012. március 23. Forrás: az Európai Bizottság (a 29. cikk szerinti munkacsoport titkárságának) honlapja. *Edpb.europa.eu.*

[274] Az Európai Bizottság által 2020. június 24-én nyilvánosságra hozott dokumentumai: *A Bizottság közleménye az Európai Parlamentnek és a Tanácsnak, A polgárok szerepe erősítésének és az EU digitális átállással kapcsolatos megközelítésének pillérét képező adatvédelem – az általános adatvédelmi rendelet alkalmazásának két éve*. COM(2020)264 végleges. 6.; *Commission Staff Working Document, Accompanying the Document: Communication from the Commission to the European Parliament and the Council, Data Protection as a Pillar of Citizen's Empowerment*

Fentebb utaltam rá, hogy a Rendelet 22 pontban határozza meg a hatóságok feladatait. A felügyeleti hatóságok jellemzően 50–200 fős létszámmal látják el teendőiket.

> Testületi állásfoglalás a GDPR értékeléséről, 26–27. A német hatóságok által összesen foglalkoztatott köztisztviselők száma kiemelkedik, mintegy ezer fő, a lengyel (260 fő), a francia (225 fő), a spanyol (220 fő) a legnagyobbak közé tartozik, a középmezőnyben helyezkedik el például az ír (176 fő) vagy a magyar (117 fő), végül például az osztrák (34 fő), a görög (46 fő) vagy a portugál (27 fő) kifejezetten kis méretű hatóság.[275]

A számok arra utalnak, hogy a 22 feladat ellátása egy ambiciózus elvárás a jogalkotó részéről. Félő, hogy a sok kötelezettség szükségszerűen vezethet egyes feladatok elhanyagolásához, annak ellenére, hogy a jogalkotó nem súlyoz fontosak és kevésbé fontosak között. A hatóságoknak ebből kifolyólag nincs lehetőségük egyes feladatokat előrébb, másokat pedig hátrébb sorolni.[276] Ez a különbségtétel pedig véleményünk szerint nélkülözhetetlen a napi teendők ellátása során. Ahogyan Raab és Székely rámutat, az adatvédelmi hatóságok személyi állománya is jelentősen befolyásolja a hatóságok mozgásterét. Írásukban a szerzők a hatóságok szűkös IT-szakértői állományára is rámutatnak, és egy lehetséges megoldásként azt a javaslatot is megfogalmazzák, hogy a szakértőket nemcsak egy hatóság, hanem más hatóságok is igénybe vehetnék, ilyen módon is csökkentve a véges források hatékonyabb felhasználását. Jegyezzük meg azt is, hogy az ilyen jellegű együttműködés a hatóságok közötti különbségek csökkentését is hatékonyan szolgálhatja.[277]

Amikor feladatok között súlyoznak a hatóságok, óhatatlanul értékítéletet is alkotnak fontosabb és kevésbé fontos feladatok között. Amellett, hogy a Rendelettel koncepcionálisan összhangban álló kockázatarányos megközelítést alkalmazhatják, adódik a kérdés, hogy a hatóságok milyen közérdeket, értéket *(public value)* tudnak felmutatni, illetve szolgálni. Moore

and the EU's Approach to the Digital Transition – Two Years of Application of the General Data Protection Regulation. (SWD2020)115 final. 12–14.

[275] *Contribution of the EDPB to the Evaluation of the GDPR under Article 97,* elfogadva: 2020. február 18-án.

[276] A tagállamokban a hatósági eljárásokra vonatkozó szabályok határozzák meg ennek rendjét, illetve korlátait.

[277] Lásd erről bővebben: Raab–Székely (2017): i. m.

elismeri, hogy a privát szférával ellentétben *(private value)* a közszférában a szolgált értékek azonosítása és mérése nehézkesebb. Nem elég azt bemutatni, hogy közös értékeket sikerrel szolgálnak a hatóságok, hanem azt is, hogy a társadalom részéről az erőforrások rendelkezésre bocsátása révén a kívánatos eredményt elérték.[278]

A hatékonyság előfeltétele, hogy a felügyeleti hatóságok rugalmasan határozhassák meg prioritásaikat. A Rendelet ebben a tekintetben tilalmat ugyan nem tartalmaz, a feladatok hosszú katalógusa mégis arra vezet, hogy egy erőteljes teljesítményelvárás érvényesül a hatóságokkal szemben, nevezetesen az, hogy minden feladatukat magas szinten el tudják látni. Attól függetlenül, hogy a tagállami kormányzatok a megfelelő forrásokat biztosítják-e, vagy sem, végig kell gondolni, vajon milyen módon tehető a rendeleti szabályoknál hatékonyabbá a hatóságok munkája.

A hatékonyság növelésére számos vezetési, irányítási eszköz áll rendelkezésre. Úgy ítélem meg, hogy nem a jelen elemzés tárgya ennek megvitatása. Az elemzés során azzal a feltételezéssel dolgozom tovább, hogy a tagállami felügyeleti hatóságok vezetése minden rendelkezésre álló eszközt igénybe vesz annak érdekében, hogy a hatóságok az adott humán és anyagi erőforrással a lehető leghatékonyabb módon lássák el feladataikat. Moore a stratégiai tervezés során az úgynevezett stratégiai háromszöget ajánlja a hatóságok vezetésének figyelmébe. A „háromszög" egyik pontja a szervezet céljának vagy küldetésének meghatározása, a második a társadalmi forrásokat és a mögöttes legitimációt veszi számba, a harmadik pedig arra utal, hogy az elérendő célok érdekében miképpen szervezi meg a szervezet belső feladatait.[279] A hatékonyság terén az útkeresés másik irányát vizsgálom.

A hatóságok új szemléletű feladatellátása

A Rendelet egyenrangú feladatokat határoz meg, ezek között pedig kiemelt szerep jut az érintetti panaszok kezelésének. A Rendelet nevesíti is azt, hogy az érintett jogosult a felügyeleti hatósághoz panasszal fordulni. A Rendelet 77. cikke szerint minden érintett jogosult arra, hogy panaszt tegyen egy felügyeleti hatóságnál, ha megítélése szerint a rá vonatkozó személyes adatok kezelése megsérti a Rendeletet. A hatóság köteles tájékoztatni az ügyfelet

[278] Moore (1995): i. m. 28–29.
[279] Moore (1995): i. m. 70–71.

a panasszal kapcsolatos eljárási fejleményekről és annak eredményéről. A hatóságoknak az egyedi panaszügyek intézését illetően nincsen mérlegelési joguk, a panasz tárgyát a szükséges mértékben kivizsgálják.[280] Colin J. Bennett és Charles D. Raab is teljes természetességgel állapítják meg, hogy az adatvédelmi hatóságok hagyományos és fontos feladata a panaszok kivizsgálása, ami „a hatékony adatvédelmi felügyelet középpontjában áll, még akkor is, ha időigényes és jelentős forrásokat emészt fel".[281] A klasszikus megközelítés szerint az adatvédelmi hatóság minden beérkező panaszt kivizsgál.

A felügyeleti hatóságok által e körben ellátott feladatok mennyisége tehát nagymértékben függ a beérkező panaszok számától, erre a hatóságoknak nincsen befolyása. A statisztikák azt mutatják, hogy még a közepes méretű hatóságok is évente ezres nagyságrendben kapnak panaszokat.[282]

A német hatóságokhoz (tartományi és szövetségi szinten) mintegy 67 ezer, a holland hatósághoz 37 ezret meghaladó, a spanyolhoz 18 ezernél is több panasz érkezett 2018. május 25-től 2019. november 30-ig. A megjelölt időszakban az osztrák hatóság majdnem 4 ezer, a magyar 3781, a portugál pedig mintegy 1400 panaszt kapott.

A panasztételhez való jog erős jogosultsága az érintettnek, amely az adatvédelmi szabályozások jelentős vívmánya. Az érintettek többsége tudja is, hogy melyik hatósághoz lehet fordulni. Az Eurobarometer 2019-es felmérése szerint arra a kérdésre, hogy hallott-e a saját országában az adatvédelemért felelős hatóságról, 57% igennel válaszolt. Ez a 2015-ös értékhez képest 20%-os javulás, amely jól valószínűsíthetően a Rendelet ismertségének is betudható. A panasz azt jelzi, hogy a magánszféra védelme terén hiányosságot észlelt az érintett, és ennek a hatóság előtt ingyen, bármikor hangot is adhat. Egyszerű és könnyen elérhető jogorvoslatról van szó. Mindazonáltal minden egyes panasz azt jelzi, hogy az adatkezelő vagy ténylegesen jogszabályellenesen járt el, vagy legalábbis nem sikerült olyan módon teljesíteni az érintettek elvárásait, amely a konfliktust elkerülhetővé vagy az adatkezelő és az érintett között rendezhetővé tette volna. Ennek okait érdemes

[280] A Rendelet 57. cikk (1) bekezdés f) pontja szerint.

[281] Bennett–Raab (2006): i. m. 135.

[282] *Contribution of the EDPB to the Evaluation of the GDPR under Article 97,* elfogadva: 2020. február 18-án. 31–32.

vizsgálni, hiszen ettől is függ, hogy a Rendelet által megalkotott rendszer milyen hatékonysággal működik.

Egyik oldalon a panasztételhez való jog erős jogosultság, másik oldalon pedig annak jele, hogy a Rendelet nem megfelelően érvényesül. E két jelenség kéz a kézben jár egymással. Azt állíthatjuk, hogy a jogalkotói cél a minél kevesebb jogsértés, ebből következően pedig a panaszok száma ideális esetben alacsony. Az adatvédelmi felügyeleti hatóságok magas számú panasz esetén egyre inkább panaszok vizsgálatával foglalkoznak.

A holland adatvédelmi hatóság (Autoriteit Persoonsgegevens) a honlapján nyilvánosságra hozott statisztika szerint 2019 első felében több mint 19 ezer megkeresést kapott állampolgároktól és különböző szervezetektől, ezek közül 15 ezernél is több panaszt iktattak és bíráltak el. Ez a 15 ezres szám több körülmény miatt is magas. Egyrészt a 17 milliós országban majdnem minden ezer lakosra jut egy adatvédelmi tárgyú panasz, másrészt Hollandiában az adatvédelmi hatóság a Rendeletet megelőzően általában nem foglalkozott egyéni panaszokkal. A 140 fős hatóságot az ekkora mennyiségben érkező panaszok értelemszerűen jelentősen leterhelik.[283]

Felmerül a kérdés: milyen módon lehetne elérni azt az állapotot, hogy a panaszok száma csökkenjen, és ez együtt járjon az adatvédelmi jog hatékonyságának javulásával? Ez abban az esetben fordulhat elő, ha az adatkezelők oldalán kevesebb ok adódik a panaszok előterjesztésére. Más szóval: megvalósul az a jogalkotói cél, hogy a magánszféra erős védelemben részesül, érvényesülnek a transzparenciára vonatkozó szabályok stb. Mi lehet ebben a hatóságok szerepe?

A panaszokat megelőző stratégia

A feladatok között említettem azt, hogy a hatóság „felhívja az adatkezelők figyelmét a Rendelet szerinti kötelezettségeikre". Ez a feladat nagyon sokféle megközelítésben teljesíthető. A hatóság honlapján közzétett tájékoztatóktól kezdve a képzéseken át egészen a szoros együttműködésekig terjedhet a lista.

[283] Forrás: a holland adatvédelmi hatóság honlapja. *Autoriteitpersoonsgegevens.nl*

A hatóságok munkáját végigkíséri egy kettősség, amely a jog hatékonysága szempontjából releváns kérdéseket vet fel. Akkor, amikor a hatóságnak egy konkrét ügyet el kell bírálnia, hogy az adatkezelő eljárása jogszerű vagy éppen jogellenes volt-e, akkor a hatósággal szemben természetes elvárás, hogy ezt szakértő módon meg tudja ítélni. Az egyedi döntések alapján esetjog épül, és ebből esetről esetre lehet követni a hatóság álláspontját a jognak való megfelelés terén. Az adatkezelők részéről mindig van igény arra, hogy a hatóság álláspontját ne csak a véletlenszerűen előforduló eseteket követve lehessen megismerni, hanem átfogóan is. Amennyiben az adatkezelő a Rendelet szabályait helyesen szeretné alkalmazni, akkor elvárja, hogy ebben őt a hatóság támogassa minden lehetséges módon. Ilyen eszköz lehet a mintaszabályzat, az adatkezelőket segítő kézikönyvek közzététele, rugalmas konzultációs lehetőséget biztosító hatósági ügyfélszolgálatok stb.

Sparrow amellett érvel, hogy hasznos azokat a mintákat vizsgálni, ahol a jognak való meg nem felelés *(non-compliance)* koncentráltan fordul elő. A hatóságok, és közelebbről a szabályozó hatóságok működését vizsgálva arra mutat rá, hogy a hagyományos modell szerint azokra a társadalmi jelenségekre, ahol a jogsértések száma nagy, megpróbálnak valamilyen állami választ, reakciót adni egy intézmény révén. Akkor, amikor a szervezet hatékonyságát és szerepét vizsgáljuk, Sparrow elemzi azt, hogy lehet egyrészt javítani, hatékonyabbá tenni a szervezet belső folyamatait. Ez járhat a hatékonyság javulásával. A valódi eredmény véleménye szerint azonban nem a panaszok kezelése, hanem azok megoldása.[284] A stratégiai problémamegoldás nem a panaszokra, hanem a valódi társadalmi probléma megoldására irányul. Sparrow az Amerikai Egyesült Államokban működő Occupational Safety and Health Administration (OSHA) példáját hozza fel, amelynek létezését kétségbe vonták, mondván, az „ipar hátán" működik, de a sajtóban megjelent elemzés a balesetek, halálesetek, megbetegedések számának jelentős csökkenésével illusztrálta a hatóság valódi társadalmi problémamegoldó képességét.[285]

Elemzésemet Sparrow véleményével egyetértve folytatom, a magam részéről is fontosnak tartva a különbségtételt. Abban az esetben, ha a hatóság nem a panaszokat követő, hanem a panaszokat megelőző stratégiát követ, sokkal nagyobb hangsúly jut az utóbbi feladatoknak. Sőt ez a kettő,

[284] Malcolm K. Sparrow: *The Character of Harms: Operational Challenges in Control*. New York, Harvard University Press, 2008. 47–71.
[285] Forrás: *The Washington Post* honlapja.

a panaszokat megelőzni hivatott, az adatkezelőket támogatni szándékozó feladatkör, valamint a panaszkezelés gyakorlatilag el is válhat egymástól. Két, egymástól lényegesen eltérő feladatról van szó, azzal együtt természetesen, hogy a hatóság mindig, minden jogkérdésben csak egyféleképpen értelmezheti a jogszabályokat. Sparrow a kockázatokkal együtt is azt a modellt javasolja, hogy elkülönített személyzet foglalkozzon ezekkel a típusú feladatokkal.

> Az egyik kockázat, hogy a külön szervezeti egységnél dolgozó munkatársak idővel elveszíthetik a tereptapaszalatot, ezért Sparrow azt a modellt is működőképesnek tartja, hogy az egyes szakértőknek vegyes portfóliót alakítanak ki. Egy másik lehetséges szervezeti-személyzeti kockázat abban mutatkozik meg, hogy míg a megszokott rutin szerint dolgozik a kollégák egy része, a többi hosszú ideig olyan feladatokat lát el, amelyek nem eredményeznek látható változást. Sőt az is kockázatként jelentkezik, hogy az új, problémafeltárásra és -megoldásra átirányított kollégák azzal szembesülnek, hogy sok olyan kreativitást igénylő feladatot kell megoldani, amelyre nincs általános iránymutatás, ellentétben a megszokott ügymenettel, és ezért visszakívánkoznak eredeti munkakörükbe.[286]

A szervezeti megoldástól függetlenül követelmény marad az egységesség a Rendelet alkalmazása során. A Rendelet egységes alkalmazásának kötelezettsége a tagállami hatóságokra egyenként és a teljes hatósági körre, testületi szinten is érvényes.

Hogyan lehet az adatkezelőket erőteljesebben támogatni a megfelelés irányába tett erőfeszítéseikben? A Rendelet megfogalmaz néhány kötelezettséget, így azt, hogy a magatartási kódexek vagy a tanúsítások alkalmazására ösztönzi az adatkezelőket. Ez a bátorító magatartás sajnálatosan kevés kézzelfogható eredménnyel járt a Rendelet alkalmazásának első két évében. A Rendelet alkalmazandóvá válásától számított két év elteltével gyakorlatilag nincsen olyan európai szintű tanúsítás, amely a megfelelő jóváhagyásokat követően az adatkezelő vagy adatfeldolgozó szervezetek számára elérhető lenne. A panaszok megelőzését is magával hozó eredményre ennél lényegesen konkrétabb és erőteljesebb lépések vezethetnek. A versenyhatóságok elismerik a jogi megfelelést ösztönző megoldások alkalmazását, és a bírságok kiszabása terén enyhítő körülményként értékelik

[286] Sparrow (2008): i. m. 149–168.

ezek helyes működését.[287] Ez a modell az adatvédelmi hatóságoknál is alkalmazható lenne.

Az adatkezelők jogszabályoknak való megfelelését támogató hatósági megközelítés gyakorlatilag a jelenleg tapasztaltakat fordítaná meg. A hatósági működésben azt látjuk Európa-szerte, hogy a panaszok nagy száma miatt a kívánatosnál sokkal kevesebb energia jut a panaszokat végső soron megelőzni hivatott programokra. A koncentrált adatkezeléssel és sok konfliktushelyzetet magában hordozó ágazatokra összpontosítva a hatóságoknak javasolt lenne olyan projekteket indítani, amelyek célja az adatkezelő kezébe megfelelést könnyítő eszközöket adni. Az adatkezelők, illetve adatkezelők szövetségei, érdekképviseleti szervei ilyen módon a hatósággal partnerségben alakíthatnák adatkezeléseiket, szabályzataikat, belső eljárásrendjüket. Ez nem azt jelentené, hogy az adatkezelő mentesül a döntéseivel járó felelősség alól, de mégis azt célozná, hogy az adatkezelő a tömeges és tipikus adatkezelések terén támaszkodhatna egy sorvezetőre. A magánszférát érintő megfontolásokon túlmutató érvek is felhozhatók e modell mellett, hiszen társadalmi szinten sokkal gazdaságosabb egy ilyen rendszer fenntartása.

A biztonsági célú kamerás megfigyelés, a munkavállalók és a munkavállalók eszközeinek ellenőrzése, a visszaélés-bejelentési rendszer, a beléptetés, a nyilvános rendezvények kapcsán kép- és videófelvételek kezelése, oktatási intézmények, kórházi adatkezelések, sütiszabályok, érintetteknek szóló típustájékoztatók, incidensbejelentések rendje, hatásvizsgálati módszertan, gyermekek nevében hozzájárulás adása – csak néhány azok közül a tömegével előforduló esetek közül, amelyekben a hatóságok általában nem, panaszügyek kapcsán azonban kénytelenek egyes jogkérdésekben állást foglalni.

A kérdést kiélezhetjük olyan formában is, hogy vajon a hatóságok birtokában vannak-e annak a tudásnak és tapasztalatnak, hogy egy ilyen szerepre vállalkozzanak? A válasz minden bizonnyal igen, hiszen az adatvédelmi

[287] Vö: A Gazdasági Versenyhivatal elnökének és a Gazdasági Versenyhivatal Versenytanácsa elnökének 11/2017. közleménye a versenykorlátozó megállapodásokra és összehangolt magatartásokra, a gazdasági erőfölénnyel való visszaélésre, valamint a jelentős piaci erővel való visszaélésre vonatkozó tilalmakba ütköző magatartások esetén a bírság összegének megállapításáról VI. fejezet 4. pontja és A Gazdasági Versenyhivatal elnökének és a Gazdasági Versenyhivatal Versenytanácsa elnökének 12/2017. közleménye a fogyasztóvédelmi típusú ügyekben kiszabott bírság meghatározásának szempontjairól VI. fejezet 2. pontja. Forrás: a GVH honlapja.

hatóságok az adatkezelésekre vonatkozóan hosszú évek alatt nagy tudást és tapasztalatot halmoznak fel. Nem a humán erőforrás felkészültsége és alkalmassága az akadálya annak, hogy egy ilyen modellre átálljanak az adatvédelmi felügyeleti hatóságok, hanem a Rendelet megközelítése. E megközelítés ugyanis abba az irányba tereli az adatkezelő-adatalany-hatóság hármasának együttműködését, hogy a felelősséget elsősorban az adatkezelőkre telepíti.

Az adatkezelők működésük során igénybe vehetnek bizonyos önkéntes megfelelési eszközöket (magatartási kódex, tanúsítás), továbbá új, kötelezően igénybe veendő jogintézményeket (incidensbejelentés, adatvédelmi hatásvizsgálat), de a szabályozás és a hatóság tulajdonképpen magára hagyja az adatkezelőket és az adatalanyokat, számonkérik az elszámoltathatóság érvényesülését. Nem amellett érvelek, hogy a hatóságoknak gyámkodnia kellene az adatkezelők fölött. Szó sincs erről. De az olyan jogkérdésekben és szervezeti-igazgatási kérdésekben, amelyek tömegével fordulnak elő a napi gyakorlatban, szükséges lenne az új szerepfelfogás szerinti hatósági működés.

Az új modell minőségi előrelépést jelentene a jelenlegi hatósági működéshez képest, és ebben rejlik az az értéke, amely a védelmi lépcső eszközével is értékelhető. Az adatalanyok oldalán ez a modell azt ígéri, hogy az adatkezelők nagyobb eséllyel fognak nemcsak jogkövető, hanem jogi kérdésekben tájékozott módon eljárni. E két kitétel némiképp eltér egymástól, de összefügg. A professzionálisabb adatkezelői eljárás és az érintetti jogok érvényesítése nem választható el egymástól. Az adatkezelő oldalán a jogbiztonság erősödik, és a munkatársak felkészítéséhez is fogódzók kereshetők a hatósági iránymutatásokban. A modell a hatóságok számára azért jelentene könnyebbséget, mert jól kalkulálhatóan – egy bizonyos átmeneti időszak után – csökkenne a panaszok száma. Egyszerűen azért, mert a tipikus konfliktusos helyzetekben az adatkezelők megnyugtató válaszokat tudnának adni mind a munkavállalóiknak, mind a többi érintettnek. Ezen a ponton el is jutunk oda, hogy ez a tendencia egy pozitív spirált indít el, ugyanis a modell helyes működése további erőforrást szabadít fel a hatóságoknál, amelyek jó hatásfokkal a tárgyalt programokban hasznosíthatók.

Útjában áll-e a Rendelet annak, hogy a tagállamok egy ilyen modellt kialakítsanak? A kérdésre adható rövid válasz nemleges, ugyanakkor a Rendelet a hatóságok feladat- és hatáskörét illetően nagyon konkrét szabályozást nyújt. A tagállami szinten bevezethető modell csak úgy lenne összhangban a Rendelettel, ha a kötelező feladatokat is ellátná az új felfogás mellett

működő hatóság. Ezen a téren a tagállami jogalkotónak nincs mozgástere. A hatóságokat elárasztják panaszokkal. A panaszok fontos jelzések a polgárok részéről, de magas számuk a rendszer nyilvános kudarcát jelzik. Véleményem szerint az ördögi körből az általam javasolt modell révén vezethető ki az adatvédelmi hatóság.

Ismét Sparrow munkájából idézve[288] a modell újításának tulajdonságai között említem, hogy mindig konkrét, jól körülhatárolt problémákra fókuszálnak a programok; hosszú elemzés előzi meg a programok bevezetését; az új intézkedések mindig újítást tartalmaznak, nem rutinszerűen épít korábbi mintákra; az új intézkedések több hatóság munkájának összehangolása révén vezetnek eredményre.

Az általam bemutatott modell működésének dinamikáját alapul véve az prognosztizálható, hogy a működés első éveiben ugyan többletforrásigénnyel járna, hiszen új feladatként jelenne meg a panaszokat megelőző stratégia végrehajtása, és a panaszokat kötelező módon továbbra is kezelni kellene. Onnantól kezdve azonban, amikor a stratégia már érezteti hatását, és a panaszok száma csökkenni kezd, a szükséges személyzettöbblet is csökkenést mutat majd. Ennek kedvező hatása nem elsősorban és nem csupán a költségek csökkenésében mérhető, hanem a magánszféra körében megvalósuló jogsértések számának csökkenésében ragadható meg. Társadalmi szinten viszont jelentős anyagi megtakarítást eredményezhet a modell alkalmazása. A jog hatékonyságának körében tett kitérő alapján ez az érdemi értéke és többlete az új modellnek.

A felügyeleti hatóságok hatásköre

A Rendelet az adatvédelmi felügyeleti hatóságok hatáskörét hármas tagolás szerint vizsgálati, korrekciós, valamint engedélyezési és tanácsadási kategóriába sorolja. A jogalkotó szándéka szerint nemcsak a feladatok, hanem a hatáskörök tekintetében is teljes a harmonizáció,[289] így a következőkben elemzendő hatáskörök minden tagállam esetében azonosak.

[288] Sparrow (2008): i. m. 64–65.

[289] Vö. a Rendelet (123) preambulumbekezdésével, ahol a jogalkotó azon szándékát jelöli meg, hogy a felügyeleti hatóságok szerepüket úgy töltik be, hogy azzal hozzájárulnak a Rendelet egységes alkalmazásához.

Vizsgálati hatáskörök

A Rendelet tíz vizsgálati hatáskört említ. Ezeket a következő öt szempont szerint csoportosíthatjuk:

1. A jogszabályellenes adatkezelések megakadályozása, megszüntetése, illetve szankcionálása kontextusában az első helyen áll a tények feltárását szolgáló vizsgálati hatáskör. Időrendben haladva az első helyen említendő hatáskör szerint a hatóság értesíti az adatkezelőt a Rendelet feltételezett megsértéséről.[290] A vizsgálat körében a felügyeleti hatóság utasíthatja az adatkezelőt,[291] illetve képviselőjét, hogy számára a feladatai elvégzéséhez szükséges tájékoztatást adja meg.[292]
2. A hatóság jogosult adatvédelmi auditok keretében vizsgálatot folytatni.[293] Az „audit" nem azonos a magyar adatvédelmi hatóság által 2018 előtt elvégzett adatvédelmi audit szolgáltatásával, hanem a tagállamokban általánosan bevett kifejezésként a hatóságok vizsgálati tevékenységére utal, a közhatalom gyakorlásának keretében – és nem önkéntesen vállalt, ellenérték fejében végzett szolgáltatásként, amelyre a NAIH adatvédelmi audit eljárása irányult.[294]
3. A kért tájékoztatáson túl a hatóság az adatkezelés helyszínén is tájékozódhat az adatkezelés körülményeit illetően. Ennek keretében hozzáférést kap az adatkezelőtől minden olyan személyes adathoz és információhoz, amelyre feladatainak ellátásához szüksége van.[295] Annak megítélése, hogy a feladatainak ellátásához egy bizonyos adathoz szüksége van-e a hatóságnak, a hatóság feladata és felelőssége. Az adatok igénylésének, illetve hozzáférésének a jogszerűsége

[290] A Rendelet 58. cikk (1) bekezdés d) pontja.

[291] A Rendelet az adatkezelőt és az adatfeldolgozót mindenhol együtt említi. Csupán az adatkezelőt jelölöm meg, azzal természetesen, hogy az elemzett szabályok az adatfeldolgozóra is irányadók.

[292] A Rendelet 58. cikk (1) bekezdés a) pontja szerint.

[293] A Rendelet 58. cikk (1) bekezdés b) pontja.

[294] Az adatvédelmi audit a NAIH gyakorlatában évekig fontos szerepet töltött be egyfajta hatósági tanúsításként. Az auditot a NAIH az adatkezelő kérésére díj ellenében végezte el, és a megfelelésről igazolást adott. A jogintézményt az Országgyűlés a Rendeletnek való megfelelésre irányuló jogalkotás során megszüntette, és hatályon kívül helyezte az Infotv. 69. §-át, az adatvédelmi auditra vonatkozó szabályokat.

[295] A Rendelet 58. cikk (1) bekezdés e) pontja.

ugyanúgy bírósági felülvizsgálat tárgya, mint minden más eljárási cselekmény.

4. Külön szabályozza a jogalkotó az adatokhoz és információkhoz való hozzáférésen túl az adatkezelő bármely helyiségéhez, felszereléséhez és eszközéhez való hozzáférést.[296] A hatóság eljárása során nem csupán az adatkezelő nyilatkozatára kénytelen hagyatkozni ilyen módon, hanem munkatársai révén a hatóság közvetlenül tud adatokba betekinteni, folyamatokat megvizsgálni, adatbiztonsági intézkedéseket értékelni stb. Jelentős beavatkozást jelent ez a hatáskör az adatkezelő tevékenységébe, ugyanakkor a technológiai környezetre, az adatok digitális tárolására való tekintettel nélkülözhetetlen ennek a hatáskörnek a biztosítása.
5. A Rendelet a vizsgálati hatáskörök között említi a tanúsítványok felülvizsgálatát.[297] A tanúsítványnak való megfelelés az adatkezelő oldalán nem mentesít ugyan a Rendelet szabályainak alkalmazása alól, mindazonáltal jelentős jogbiztonságot nyújt az esetleges jogsértések gyanúja esetén. Ez az önkéntesen választható elszámoltathatósági eszköz azonban csupán meghatározott időre szól,[298] háromévente felül kell vizsgálni. Ha a tanúsítványra vonatkozó követelmények már nem teljesülnek, akkor a tanúsítványt vissza kell vonni. Ezt a tanúsítószervezet vagy a hatóság teheti meg.[299] Adódhatnak olyan helyzetek, amikor a tanúsítószervezet például megszűnik, vagy egyébként jogellenes módon nem vonja vissza a tanúsítványt, pedig annak helye lenne. Ilyenkor a tárgyalt hatáskörével a hatóság maga is élhet, ilyen módon biztosítva, hogy a tanúsítványokra jogellenes módon ne lehessen hivatkozni.[300]

Korrekciós hatáskörök

Korrekciós hatáskörének alkalmazása során tíz különböző jogkövetkezmény közül választhat a hatóság:

[296] A Rendelet 58. cikk (1) bekezdés f) pontja.
[297] A Rendelet 58. cikk (1) bekezdés c) pontja.
[298] Legfeljebb hároméves időtartamra lehet kiállítani – Rendelet 42. cikk (7) bekezdés.
[299] A Rendelet 42. cikk (7) bekezdés utolsó mondata szerint.
[300] Ezzel a hatáskörével a Hatóság még nem élt – működő tanúsítás hiányában.

1. Még meg nem történt, de valószínűsíthető jogsértés esetén figyelmeztetést alkalmazhat

Az adatvédelmi hatóság figyelmezteti az adatkezelőt, ha tervezett adatkezelése valószínűsíthetően sérti a Rendelet szabályait.[301] Jogsértés még nem valósult meg, a hatóság mégis, már ebben a fázisban korrekciós hatáskörében léphet fel. A Rendelet nem szól arról, hogy a hatóság milyen módon jut az információk birtokába, ez gyakorlatilag irreleváns, a jogalkotó itt nem ír elő semmilyen korlátozást. Az egyik lehetséges módja, hogy adatvédelmi hatásvizsgálat[302] keretében kezdeményez az adatkezelő előzetes konzultációt a hatósággal, és így jut a hatóság tudomására a tervezett adatkezelés.

A figyelmeztetés nem jelent tilalmat, és a hatóság feltételezése, amely szerint a Rendelet szabályai sérülhetnek, nem feltétlenül olyan precízen kimunkált, mint például egy adatkezelést megtiltó döntése. Erre utal a „valószínűsíthetően" kitétel, a norma tekintettel van az adatkezelés még csak tervezett voltára.

2. Megtörtént, de bírság kiszabását nem minden esetben igénylő jogsértés esetén elmarasztalja az adatkezelőt vagy az adatfeldolgozót

Adatfeldolgozó az a személy, aki az adatkezelő nevében személyes adatokat kezel (Rendelet 4. cikk 8. pont). A gyakorlatban ez általában technikai jellegű feladatok ellátását jelenti, minden esetben adatfeldolgozói szerződés alapján. Az adatfeldolgozó köteles az adatkezelő utasításait követni, a Rendelet azonban az adatfeldolgozói felelősséget láthatóbbá teszi, és bizonyos körben maga is felelős az általa elkövetett, az adatkezelő által nem befolyásolható jogsértésekért.

A Rendelet ezekre az esetekre csupán annyit ír elő, hogy az elmarasztalás akkor alkalmazandó, amikor az adatkezelő adatkezelési tevékenységével megsértette a Rendelet rendelkezéseit.[303] A Rendelet nem részletezi, hogy mi az elmarasztalás tartalma, de gyakorlatilag a hatóság rosszallásaként

[301] Rendelet 58. cikk (2) bekezdés a) pont.

[302] Az adatvédelmi hatásvizsgálatra irányuló eljárást a Rendelet 35. és 36. cikke szabályozza. A 36. cikkben szabályozott esetben az adatkezelő köteles a hatósághoz előzetes konzultáció igényével fordulni.

[303] Rendelet 58. cikk (2) bekezdés b) pont.

értékelendő, a jogsértés megállapítása mellett.[304] A hatóságnak nem feladata kártérítés vagy sérelemdíj ügyében állást foglalnia, azonban a jogsértést megállapító és az adatkezelőt elmarasztaló határozat bizonyítási eszközként szolgálhat például egy sérelemdíj megállapítására irányuló bírósági eljárásban.

3. Utasítja az adatkezelőt, hogy teljesítse az érintett jogai gyakorlására irányuló kérelmét, vagy arra, hogy nyújtson tájékoztatást az érintett számára az adatvédelmi incidensről

A figyelmeztetés és az elmarasztalás után az utasítás már tényleges és közvetlen beavatkozást jelent az adatkezelő jogaiba és kötelezettségeibe.[305] E hatáskör alapján a hatóság a jogellenes helyzetbe avatkozik bele, amelyben az adatkezelő nem teljesítette az érintett Rendeletben rögzített valamely jogát. Az adatvédelmi incidensről való tájékoztatás azért igényel külön kiemelést a normaszövegben, mert az nem az érintett kérelmétől függ. Amikor a hatóság az itt tárgyalt hatáskörével él, akkor az adatkezelő azon mulasztását korrigálja, amely szerint az adatvédelmi incidensről az adatalanyokat tájékoztatni kellett volna. A Rendelet 34. cikke szerint a természetes személyek jogaira nézve valószínűsíthetően magas kockázattal járó adatvédelmi incidensről késedelem nélkül tájékoztatni kell az érintetteket.

4. Utasíthatja az adatkezelőt arra, hogy adatkezelését hozza összhangba a Rendelettel

A hatáskörök között minden bizonnyal ez a leginkább általános, hiszen az adatkezelési műveletek Rendelettel való összhangját szolgálja mindenféle további specifikáció nélkül.[306] A hatóság meghatározott módon és meghatározott időn belüli összhangba hozatalt is előírhat. E téren a hatóságnak széles körű mérlegelési lehetősége van,[307] a külön nevesített eseteken túl

[304] Az elmarasztalás a bírság kiszabása mellett is elképzelhető, így járt el a NAIH a NAIH/2019/1598 számú vagy a NAIH/2019/1841 ügyben is. A NAIH joggyakorlatában az számít ritkább esetnek, ha bírság nem kíséri az elmarasztalást, mint például a NAIH/2019/3114/8 számú ügyben.

[305] Rendelet 58. cikk (2) bekezdés c) pont.

[306] Rendelet 58. cikk (2) bekezdés d) pont.

[307] Azt, hogy a hatóság e hatásköre szélesen értelmezendő, a magyar bírósági gyakorlat is megerősítette a NAIH határozatainak felülvizsgálata során.

a Rendelettől való bármilyen eltérés esetén élhet az utasítás jogával. Gyakorlatilag bármilyen kötelezés jogszerű lehet, aminek alapja a Rendeletben megtalálható. Ez az utasítási hatáskör fontos eszköz a hatóságok kezében minden olyan esetben, amikor a határozat révén esély mutatkozik a jogszerű állapot megteremtésére.

5. Korlátozhatja az adatkezelést

Az adatkezelés korlátozása egy átmeneti eszköz az érintett jogainak biztosításában. (Tipikus esetként említhető, amikor a jogellenes magatartást rögzítő felvételek kezelését korlátozzák, és az adatkezelőt arra kötelezik, hogy a felvételeket a rá egyébként irányadó szabályok szerint ne semmisítse meg, annak érdekében, hogy a felvételek a felelősség megállapítása érdekében a bíróságok, hatóságok rendelkezésére álljanak.)[308] A korlátozás érdekében megjelölt adatokat például csak meghatározott célból lehet kezelni, így adott esetben bizonyítékként felhasználni. A korlátozás jellegét illetően a hatóságnak szintén széles körű mérlegelési joga van.

6. Megtilthatja az adatkezelést

A hatóság egyik legerősebb hatásköre a tilalom.[309] A tiltás eredményeként az adatkezelő az adatkezeléssel érintett adatokat nem használhatja fel azokra a célokra, amelyekre korábban – jogellenesen – felhasználta. A hatóság e hatáskörével az arányosság figyelembevételével él, a tilalom esetén ez a követelmény különösen hangsúlyozandó, hiszen egy adatkezelő szervezet üzleti tevékenységét lehetetlenítheti el a tilalom alkalmazása. Határt kell vonni a büntetés és a jogellenességet korrigáló hatáskörök között, a tilalom pedig korrekciót szolgál, értelemszerűen nem alkalmazható büntető jelleggel. Amennyiben az adatkezelés egyéb módon összhangba hozható a Rendelet szabályaival, a tilalom alkalmazása aránytalan intézkedésnek tekintendő.

[308] A hatáskört a Rendelet 58. cikk (2) bekezdés f) pontja szabályozza, míg az adatkezelés korlátozásának definícióját a 4. cikk 3. pontja rögzíti.

[309] A Rendelet 58. cikk (2) bekezdés f) pontjának második fordulata szerint élhet a hatóság e hatáskörével.

7. Elrendelheti az adatok helyesbítését, törlését, valamint az érintetti jogok gyakorlása kapcsán azon címzettek értesítését, akikkel a személyes adatokat közölték

Az adatkezelés korlátozásához és tilalmához hasonlóan e hatáskör gyakorlása során a hatóság közvetlenül avatkozik bele az adatok kezelésébe, arra nézve konkrét kötelezést alkalmaz.[310] A hatóság ilyen esetekben felléphet érintetti kérelem alapján is, azonban attól függetlenül is, tehát minden olyan esetben, amikor a Rendelettel való összhang megteremtése ezt indokolja. A törlés végleges, visszavonhatatlan műveletet jelent, ennek kapcsán ismét utalunk az arányosság követelményére.

Az elfeledtetéshez, a helyesbítéshez, a törléshez, valamint az adatkezelés korlátozásához való jog érvényesüléséhez elengedhetetlen, hogy a szükséges műveleteket minden olyan adatkezelő végrehajtsa, aki az adatok birtokába jutott. Ennek érdekében ruházta fel a jogalkotó a hatóságot azzal a hatáskörrel, hogy az adatkezelőt e kötelezettségének teljesítésére utasítsa. Itt ismét tipikusan korrekciós hatáskörről beszélünk, hiszen az adatkezelőnek a hatósági kötelezéstől függetlenül tájékoztatnia kellene ilyen esetekben az említett adatkezelőket.[311]

8. Visszavonhatja a tanúsítványt, vagy a tanúsítószervezetet utasítva visszavonatja a tanúsítványt; utasíthatja a tanúsítószervezetet, hogy a tanúsítványt ne adja ki

E ponton utalok a Rendelet 42. cikk (7) bekezdése kapcsán a vizsgálati hatáskörnél már elmondottakra,[312] ahol bemutattam a hatóság azon hatáskörét, amely szerint visszavonhatja a tanúsítványt. A Rendelet szabályozása szerint a tanúsítószervezet tanúsítvány kibocsátásához való joga összefonódik a hatóság tanúsítvánnyal összefüggő hatásköreivel. Minden ponton érvényesül a hatóság beavatkozási lehetősége, hiszen nemcsak a tanúsítvány kibocsátását tilthatja meg a tanúsítószervezet számára, hanem elvégezheti a tanúsítvány felülvizsgálatát, majd pedig a felülvizsgálat fényében a hatóság

[310] A Rendelet 58. cikk (2) bekezdés g) pontja.

[311] A vonatkozó kötelezettségeket a Rendelet 16., 17., 18. és 19. cikkei tartalmazzák, amelyek kiegészülnek a tárgyalt hatáskört rögzítő 58. cikk (2) bekezdés g) pontjával.

[312] A tanúsítvány visszavonására vonatkozó, a 42. cikk (7) bekezdésében rögzített hatáskört az 58. cikk (2) bekezdés h) pontja megismétli.

dönthet arról, hogy a tanúsítványt ő maga visszavonja, és erre nem a tanúsítószervezetet utasítja. A tanúsítvány tehát, mint önszabályozó eszköz, erős hatósági kontroll mellett működik.

9. Közigazgatási bírságot szabhat ki

Közigazgatási bírságot a többi szankció alkalmazása mellett vagy azok helyett is kiszabhatnak.[313] Az eljáró hatóság felelőssége arról dönteni, hogy alkalmaz-e szankciót az adott eljárás során, és amennyiben így dönt, akkor a lehetséges jogkövetkezmények közül melyiket, illetve melyek kombinációját alkalmazza.

A közigazgatási bírság tipikusan büntető jellegű szankció, nem feltétlenül csupán korrekciós szerepe van.[314] A hatáskörök között az elmarasztalás és a bírság az, amely egyfajta értékítélettel társul, tehát a hatóság rosszallása, illetve a speciális és generális prevenciót szolgáló törekvése megnyilvánul. A közigazgatási bírságról lentebb külön fejezetben szólok.

10. Elrendelheti a harmadik országbeli címzett vagy nemzetközi szervezet felé irányuló adattovábbítás felfüggesztését[315]

Az adattovábbítás tilalma szintén tipikusan kiigazító jellegű hatáskör,[316] alkalmazására akkor kerülhet sor, amikor az adatkezelő nem tesz eleget az egyébként rá nézve alkalmazandó kötelezettségének, és ebben az esetben hatósági közbelépés szükséges. Számos olyan eset elképzelhető, amikor a hatóság e hatáskörét gyakorolhatja. Így például érintetti panasznál abban az esetben, ha az adattovábbítás alapja az érintetti hozzájárulás volt, amelyet az adatalany időközben visszavont; előfordulhat, hogy az adatvédelem megfelelő szintjének garanciája megszűnik, és emiatt kell – még megfelelő jogalap megléte esetén is – felfüggeszteni az adattovábbítást.

[313] A Rendelet 83. cikk (2) bekezdésének első mondata szerint.
[314] A Rendelet 58. cikk (2) bekezdés i) pontja rögzíti ezt a hatáskört, annak részleteit a 83. cikk rögzíti.
[315] A Rendelet 58. cikkének (2) bekezdése alapján.
[316] A hatáskört a Rendelet 58. cikk (2) bekezdés j) pontja rögzíti.

A Safe Harbor jogi keretét biztosító európai bizottsági határozat hatályon kívül helyezését követően különös jelentőséggel merült fel kérdés az Amerikai Egyesült Államokba irányuló adattovábbítások jogszerűsége kapcsán. Az Európai Unió Bíróságának 2015. október 6-án született, hatályon kívül helyező ítéletét követően a megfelelőséget biztosító határozat általános kerete helyett az adatkezelések egyedi jogszerűségét biztosító jogi eszközöket kellett alkalmazni. Az adatkezelések jogszerűségét szolgálhatta például a kötelező erejű vállalati szabályok és a standard szerződéses kikötések alkalmazása. Ezen a téren nyújtott iránymutatást a 29-es adatvédelmi munkacsoport 2015. október 16-án kibocsátott állásfoglalása a Data Protection Commissioner kontra Facebook Ireland Ltd, Maximillian Schrems ügyben, amelyet Schrems II döntésként is szokás említeni. A Safe Harbort felváltó úgynevezett Privacy Shield rezsimet érvénytelennek nyilvánította a Bíróság.[317]

A lehetséges esetek sora folytatható lenne, mindegyikben közös azonban, hogy e hatáskör gyakorlása szorosan összekapcsolódik a védelem szintjével. A harmadik országba irányuló adattovábbítás esetében ugyanis az adattovábbítás jogalapja nem elégséges feltétele az adatkezelésnek, emellett a megfelelő védelmi szintet is szavatolni kell. Ha bármelyik feltétel hiányzik, az adattovábbítás, valamint az adatok harmadik országban történő további kezelése jogellenessé válik. Fontos beavatkozási lehetőség tehát ez a hatáskör a hatóságok számára, hogy az érintettek jogainak védelmében fel tudjanak lépni.

Az Európai Unió Bírósága az úgynevezett Schrems-ügyben, előzetes döntéshozatali eljárás keretében hozott ítéletében hangsúlyozta az adatvédelmi felügyeleti hatóságok szerepét abban, hogy a harmadik országba irányuló adattovábbítások jogszerűségét akkor is vizsgálhassa, amikor egyébként az Európai Bizottság határozatában megállapította egy harmadik ország vonatkozásában a megfelelő védelmi szint meglétét. Ennek hiányában ugyanis a hatóságok azon jogosultsága, hogy az Európai Unióból induló adattovábbítások jogszerűségének körülményeit vizsgálhassa, kiüresedne.[318]

[317] Az Európai Unió Bíróságának ítélete, C-311/18. sz. ügy, ECLI:EU:C:2020:559.
[318] Case C-362/14 Maximilian Schrems v. Data Protection Commissioner, az ítélet kelte: 2015. október 6.

Ennek a védelmi szintnek a fenntartása az Európai Unió Bíróságának gyakorlatában is megjelenik, a bírósági joggyakorlat ebben a tekintetben következetes.

Az Európai Parlament kutatási szolgálata (European Parliament Research Service) által készített *From Safe Harbor to Privacy Shield – Advances and Shortcomings of the New EU-US Data Transfer Rules* című tanulmánya rámutat arra, hogy a Schrems-ítélet az EUB már kialakított standardját erősítette meg. Az Európai Unió adatmegőrzési irányelvét érvénytelenné nyilvánító Digital Rights Ireland-ítéletben az EUB szintén az EU Alapjogi chartájára tekintettel elemezte a jogkorlátozás mértékét. Az Alapjogi charta fényében a bíróság arra jutott, hogy a beavatkozás mértéke különösen súlyos. Ehhez hasonlóan a Schrems-ügyben is arra a következtetésre jutott a bíróság, hogy a jogkorlátozás nem szorítkozik a szigorúan szükséges mértékűre. Éppen ellenkezőleg, az adatok továbbítása számos alapelvi szabályt sért, amikor hiányoznak az adatok további felhasználásának korlátait jelentő objektív követelmények, a kivételek és az adatkezelés jól körülhatárolt céljai.

Az adatvédelmi hatóságok eljárásaival szemben támasztott uniós jogi követelmények

Jelen írásnak nem célja, hogy az adatvédelmi felügyeleti hatóságok tagállami szinten folytatott eljárásait részletesen elemezze. A közös hatáskörgyakorlás egyes aspektusait elemzem az alábbiakban. Az eljárásokkal kapcsolatos általános elvárások említése mégis inkább e fejezetbe kívánkozik, hiszen alapvetően a tagállami, nem együttműködési, illetve egységességi eljárások szabályozása volt a jogalkotói cél e követelmények Rendeleti szintű rögzítésével.

A tagállami eljárási jogok követelményrendszerén túl maga a Rendelet is támaszt elvárásokat az eljárások lefolytatásával, a hatóságok intézkedéseivel kapcsolatban.[319] Magától értetődő általános elvárás, hogy a hatóságok hatásköreiket „megfelelő garanciák" mellett gyakorolják, további elvárás a pártatlanság és a tisztességes eljárás, amely kiegészül a hatáskörök észszerű

[319] A Rendelet (129) preambulumbekezdése sorolja fel az általános elvárásokat a tagállami eljárásokkal szemben.

határidőn belüli gyakorlásának követelményével. Az alkalmazott intézkedésnek megfelelőnek, szükségesnek és arányosnak kell lennie. Eljárásjogi garanciaként rögzíti a meghallgatáshoz való jogot. Minden személynek joga van ahhoz, hogy az őt esetlegesen hátrányosan érintő intézkedés meghozatala előtt meghallgassa a felügyeleti hatóság.[320] Ezt egészíti ki a felesleges költség és a túlzott kényelmetlenség okozásának tilalma.

A Rendelet a tagállami eljárásjogra bízza, hogy a helyiségekbe való belépés esetén milyen eljárási garanciát várnak el a felügyeleti hatóságoktól, például a bírói engedély beszerzésének kötelezettségét. A hivatkozott (129) preambulumbekezdés tagállami eljárásjogi részletekig menően szabályozza az intézkedések (döntések) kellékeit, így előírja, hogy azokat írásban kell meghozni, világosnak és egyértelműnek kell lenniük, meg kell jelölni a dokumentumban az intézkedést hozó hatóság megnevezését, a dátumát, kötelező kellék továbbá a hatóság képviselőjének aláírása, az indokolás, és a hatékony jogorvoslathoz való jogról szóló tájékoztatás. A Rendelet azt is előírja, hogy a hatóság döntése bírósági felülvizsgálat alá vonható az adott tagállamban.

A felügyeleti hatóságok hatáskörgyakorlásának hatékonyságát szolgálja az a rendeleti rendelkezés, amely szerint a tagállami jogalkotó szabályt alkot arról, hogy a hatóság a Rendelet megsértéséről tájékoztathatja az igazságügyi hatóságokat (bíróságokat). A bíróságok előtti eljárásokat illetően a Rendelet elvárja a tagállamoktól, hogy a hatóságok önállóan indíthassanak eljárást, vagy az eljárásokban „egyéb módon", tipikusan beavatkozóként vehessenek részt. Ez utóbbi hatáskör a Rendelet hatékony érvényesülését szolgálja. A magyar adatvédelmi felügyeleti hatóság adatvédelmi ügyekben nem rendelkezik önálló keresetindítási joggal, mindazonáltal mind adatvédelmi, mind információszabadság-ügyekben élhet a beavatkozás lehetőségével. Értékelésem szerint kívánatos, hogy az adatvédelmi felügyeleti hatóságok és a bíróságok szorosan együttműködjenek, hiszen a hatósági és a bírósági szempontok kölcsönös megismerése a tagállamon belül hozzájárul az egységes jogértelmezéshez, a döntéshozatal minőségének javításához, végső soron pedig a védelem erősítéséhez.

[320] „Minden személynek joga van ahhoz, hogy az őt esetleg hátrányosan érintő egyedi intézkedés meghozatala előtt meghallgassák" – a (129) preambulumbekezdés ötödik mondata szerint.

A tagállami adatvédelmi felügyeleti hatóságok hatásköre a védelmi lépcső fényében

A felügyeleti hatóságok hatáskörének rendeleti szintű rögzítése jelentős mértékű egységesítést hozott magával. A tagállami helyett az uniós jogalkotó határozta meg a pontos és tételes listát. Hol helyezkedik el a rendeleti szabályozás a védelmi lépcsőn? Az összehasonlítás alapját ismét az irányelvben kell keresnünk, a tagállami implementációktól függetlenül.

A Rendelet közvetlenül alkalmazandó jogalkotási aktus, míg az irányelv tagállami átültetést igényel. Az összehasonlítás alapja így csalókának tűnhet, hiszen típusában két eltérő szöveget hasonlítunk össze, mégis helyesnek tartom ezt a kiindulópontot. Itt érdemes felidézni azt a kritikát, amelyet az uniós jogalkotó az adatvédelmi irányelv tagállami implementációjával kapcsolatban a Rendelet (9) preambulumbekezdésében megfogalmazott. E szerint „[…] az irányelv nem akadályozta meg sem azt, hogy az Unió tagállamaiban az adatvédelem végrehajtása széttagolt módon valósuljon meg, sem a jogbizonytalanságot, sem pedig azt, hogy széles körben az a benyomás alakuljon ki, hogy a természetes személy védelme – különösen az online tevékenységek esetében – jelentős kockázatoknak van kitéve".

Az adatvédelmi irányelv lényegében hasonló hatásköri katalógust tartalmazott, mint a Rendelet. Előírta a vizsgálati jogkör, valamint a tényleges beavatkozási lehetőségek szabályozását, ez utóbbi körben az adatkezelés megkezdése előtti véleményezés, továbbá a bírósági eljárásba való beavatkozás lehetőségét.

Az irányelv 28. cikk (3) bekezdése szerint „legalább" a következő jogosultságokkal rendelkeznek a hatóságok:
- vizsgálati jogkör, mint például az adatfeldolgozási műveletek tárgyát képező adatokhoz való hozzáférés joga;
- továbbá a felügyeleti feladatok ellátásához szükséges adatok gyűjtésének joga;
- tényleges beavatkozási jogosultságok, mint például a 20. cikknek megfelelően végzett adatfeldolgozási műveletek megkezdése előtti véleményezés joga;
- e vélemények megfelelő közzétételének biztosítása;
- az adatok zárolásának, törlésének vagy megsemmisítésének elrendelése;
- az adatfeldolgozás átmeneti vagy végleges tilalmának megállapítása;
- az adatkezelő figyelmeztetése vagy megrovása;

– illetve az ügy nemzeti parlament vagy más politikai intézmény elé terjesztése;
– bírósági eljárásban való részvétel joga az irányelv értelmében elfogadott nemzeti rendelkezések megsértése esetén;
– továbbá e jogsértések igazságszolgáltatási hatóságok elé terjesztésének joga.

Amint a feladatok listája, úgy a hatáskörök bővülése kapcsán is utalok a „mennyiségi" különbségekre is. Önmagában az, hogy az adatvédelmi hatóságok hatásköre szélesedik, olyan mozgástértöbbletet hoz, amelyet a védelem szempontjából minőségi előrelépésként kell értékelnünk. Új hatáskörök kapcsolódnak a Rendelet által bevezetett új érintetti jogok gyakorlásához,[321] a tanúsítványok és a magatartási kódexek jóváhagyásához, felülvizsgálatához,[322] az adatvédelmi incidens kezeléséhez,[323] a harmadik országbeli címzett felé irányuló adatáramláshoz.[324] A harmadik országba irányuló adattovábbítások jogszerűségének feltételeit illetően is új hatásköröket kaptak a hatóságok.[325]

A feladatok ellátásával összefüggésben egy olyan „torlódásról" is szóltam, ami a hatékonyság rovására mehet. Ilyen jelenséggel a hatáskörök kapcsán nem kell számolni, hiszen a hatáskörök teljes skálájának gyakorlása nem merül fel elvárásként. Olyan eszköz ez a kibővült hatáskör, amely az egyes eljárások során az elérni kívánt cél érdekében tetszőleges kombináció szerint alkalmazható.

Az irányelvi szabályozással összevetve a minőségi előrelépés abban ragadható meg, hogy a Rendelet a felsorolt új hatáskörök révén gyakorlatilag minden olyan életviszonyba beavatkozási lehetőséget biztosít a hatóságok révén, amely a magánszféra védelmét érintheti.

A védelmi lépcső elmélet fényében minőségi javulásként tarthatjuk számon, hogy a hatóságok bővülő hatásköre révén javul a jogérvényesítés

[321] A hatóság az elfeledtetéshez való jog kontextusában elrendelheti azon címzettek értesítését, akikkel a személyes adatokat korábban közölték [58. cikk (2) bekezdés g) pont].
[322] A vonatkozó rendelkezések az 58. cikk (1) bekezdés c), (2) bekezdés h), valamint a (3) bekezdés d), e), f) pontjaiban találhatók.
[323] Az 58. cikk (2) bekezdés e) pontja szerint a hatóság kötelezheti az adatkezelőt arra, hogy tájékoztassa az érintettet az adatvédelmi incidensről.
[324] A hatóság az ilyen adatáramlást döntésében felfüggesztheti [58. cikk (2) bekezdés j) pont].
[325] A hatóságok általános adatvédelmi kikötéseket [46. cikk (2) bekezdés d) pont] fogadhatnak el, szerződéses rendelkezéseket [46. cikk (3) bekezdés a) pont] és közigazgatási megállapodásokat [46. cikk (3) bekezdés a) pont] engedélyeznek, továbbá kötelező erejű vállalati szabályokat (47. cikk) hagynak jóvá.

lehetősége. A hatósági hatáskörök révén az érintettek mindegyikét érinti ez a minőségi javulás, hiszen nem feltétlenül egyéni kérelemhez kötött. A hatóság valamennyi érintett érdekében felléphet.

Szintén minőségi előrelépést jelent a hatáskörök tekintetében az, hogy a hatósági mozgástér bővülése világosabb szabályozási környezetet eredményez, ennek révén az adatkezelők oldalán is egyértelmű, hogy milyen esetekben kerülhet sor hatósági beavatkozásra. Az új jogintézmények, így az incidens bejelentése, a kódex, a tanúsítás szintén kiegészül szankciókkal, így biztosítva, hogy az új előírásokat nem *lex imperfecta* módon kodifikálták. Ez természetesen egy minimális elvárás, mégis jellemzi a jogalkotás minőségét.

Összességében azt állapíthatjuk meg, hogy a Rendelet új hatásköri szabályai a védelmi lépcsőn minőségi előrelépésként értékelendők, az irányelvvel való összehasonlítás, valamint a védelmi lépcső által elvárt minőségi jellemzőkkel való összevetés is ezt mutatja. A védelmi lépcső két fokát ilyen módon meg tudtuk határozni, az első a Rendeletet megelőző időszakot jellemezte, míg a második szintet maga a Rendelet jeleníti meg.

Milyen módon lehetne a védelmi lépcső következő szintjét meghatározni? Milyen minőségi vagy akár mennyiségi módosításra lenne szükség?

Álláspontom szerint a hatáskörök rendszeres felülvizsgálata és karbantartása szükségszerűen fogja a jelenlegi védelmi szintet legalábbis fenntartani, vagy újabb szintváltást nem eredményező módon megőrizni. Az elemzés arra vezet, hogy a Rendelet gyakorlata a következő években fogja majd igazolni vagy éppen cáfolni, hogy a hatáskörök katalógusa elegendő-e a hatékony jogvédelemhez. Feltételezésünk szerint erre a kérdésre igenlő választ fogunk kapni. A meglévő különbségek a tagállami közigazgatási eljárási szabályok között azonban több kérdést is felvetnek. A különböző eljárásrendek formálisnak tűnő különbségei bizonyos értelemben csupán szintén formális eljárási különbségekhez vezetnek. (A kérelmek befogadhatósága, a nyelvi kötöttségek, a panaszügyintézés menete, a határidők, a békés vitarendezés lehetőségei, az eljárás nyilvánossága, az ügyfél meghallgatása vagy az érintett eljárásjogi helyzetére vonatkozó különböző szabályok sok gyakorlati problémát okoznak.)[326] Mindazonáltal a Rendelet súlyos hiányosságának tarthatjuk, hogy az anyagi jogi szabályok mellett nagyon kevés a harmonizált eljárásjogi követelmény. A Rendelet hatékony

[326] *Contribution of the EDPB to the evaluation of the GDPR under Article 97,* elfogadva: 2020. február 18-án.

érvényesítését rábízza a tagállami jogalkotóra akkor, amikor legalább minimális eljárási szabályokat sem épít bele a kikényszerítés szabályrendszerébe. Olyan kockázatot vállal ezzel az uniós jogalkotó, amelyet önmagában is a jog hatékonyságát veszélyeztető körülményként kell számontartanunk.

A védelmi lépcsőn az jelent majd előrelépést, amikor a hatáskörgyakorlás is a tagállamok által meghatározott közös szabályrendszer szerint valósul meg. A Rendeletet közigazgatási kódexszel, vagy legalábbis minimális eljárási garanciarendszerrel kell kiegészíteni. Enélkül nem számíthatunk arra, hogy a harmonizált hatásköri lista harmonizált gyakorlathoz vezet a tagállamokban. Ennek következtében pedig egy olyan hatékonysági deficittel kell számolnunk, amely a védelmi lépcső elért fokát rendkívül törékennyé teszi. Fogalmazhatunk úgy is, hogy a Rendelet által elért védelmi szintet, már ami a hatósági hatáskörgyakorlást illeti, egy folyamatos visszacsúszás fenyegeti. Azzal is számolni kell, hogy az uniós jogalkotás a tagállami jogalkotásnál lényegesen lomhább, ezért a védelmi lépcsőn érvényesülő, felfelé mutató „gravitáció" sem képes ezt a hiányosságot olyan időn belül ellensúlyozni, hogy az ne járhatna valós védelmi veszteséggel.

Az adatvédelmi bírság

A következő fejezet az *Alkotmánybírósági Szemle* 2019. februári számában megjelent, *Az adatvédelmi bírságról – a GDPR szabályainak elemzése* című írásomon alapul.

Az Európai Unió 2018. május 25-étől alkalmazandó általános adatvédelmi rendelete számos új szabályt tartalmaz a korábbi szabályozáshoz képest. Az adatvédelmi bírság uniós szinten újdonságot jelent, ugyanakkor több tagállamban a bírság alkalmazása már korábban is a gyakorlat része volt. (Az Európai Unió Alapjogi Ügynökségének 2010-es elemzése szerint az Európai Unió 27 tagállamából 19-ben szabhatott ki bírságot az adatvédelmi hatóság. Az egyik kivétel Magyarország volt.)[327] Újdonságát az jelenti mégis, hogy – amint arról fentebb szóltunk – az egész EU területén azonos hatásköröket állapít meg az adatvédelmi felügyeleti hatóságok számára, és ennek egyik fontos eleme a közigazgatási bírság. Utaltam már rá, hogy

[327] Európai Unió Alapjogi Ügynöksége: *Data Protection in the European Union: the Role of National Data Protection Authorities – Strengthening the Fundamental Rights Architecture in the EU II.* Luxembourg, Publications Office of the European Union, 2010. 34.

a Rendelet szabályozási hiányosságokat pótol. Így van ez az adatvédelmi bírsággal is. Már a 2010-es közvélemény-kutatás során is a válaszadók legnagyobb aránya a bírság kiszabását találta a legmegfelelőbb szankciónak azokkal a vállalatokkal szemben, amelyek a felhasználók adatait jogellenesen kezelik.[328] A jogalkotói cél világos: a közigazgatási szankciók szigorítása és harmonizálása a Rendelet által előírt szabályok betartásának erősítése érdekében.[329]

A személyes adatok védelmének kontextusában értékelhetjük úgy is, hogy az uniós jogalkotó egy mércét hozott létre, ami akkor válik kitapinthatóvá, amikor a jogalkalmazó hatóság azt mérlegeli a Rendelet alapján, vajon szükséges-e a bírság kiszabása az adott ügyben. Amennyiben igen, úgy ezt a mércét a jogsértés jogi értelemben átlépte, ha pedig nem szab ki bírságot, akkor e küszöb alatt marad a jogsértés mértéke. A bírságok számának növekedésével a hatósági gyakorlat alapján tudjuk egyre pontosabban bemutatni ezt a mércét, tehát azt, hogy milyen típusú és súlyú jogsértések váltanak ki pénzügyi szankciót és melyek nem. Az alábbiakban a jogi szabályozás és az annak alapján készült európai adatvédelmi testületi[330] iránymutatást is elemzem az adatvédelmi bírságra vonatkozó szabályozás kapcsán. Az Európai Adatvédelmi Testület (a továbbiakban: Testület) tagjai egyetértettek abban, hogy az iránymutatást mint közös megközelítést alkalmazzák. Ezt az elemzést összekapcsolom a védelmi lépcső elméletével, és azt vizsgálom, hogy a közigazgatási bírságra vonatkozó új szabályozás miként értékelhető, jelent-e minőségi előrelépést a korábbi szabályozáshoz képest, és milyen lehetőség mutatkozik a további előrelépésre.

[328] Special Eurobarometer Report (359): Attitudes on Data Protection and Electronic Identity in the European Union (Az adatvédelemmel és az elektronikus személyazonossággal kapcsolatos hozzáállás az Európai Unióban). *Europa.eu/eurobarometer,* 2011. 190–193.

[329] A Rendelet (150) és (148) preambulumbekezdésének első mondatai szerint.

[330] Az Európai Adatvédelmi Testületet a Rendelet hozta létre. Elődje, a 96/46/EK adatvédelmi irányelv 29. cikke alapján létrehozott adatvédelmi munkacsoport 1995 és 2018 között számos adatvédelmi kérdésben foglalt állást, bocsátott ki véleményeket és ajánlásokat. A Rendelet alkalmazására való felkészülés során megalkotott 29-es munkacsoporti iránymutatásokat az Európai Adatvédelmi Testület első ülésén, 2018. május 25-én Brüsszelben ünnepélyesen megerősítette. Az első testületi dokumentumok között szerepelt az adatvédelmi bírságról alkotott iránymutatás is. A testület által megerősített 29-es munkacsoporti dokumentum címe: Iránymutatás a 2016/679 Rendelet szerinti közigazgatási bírság alkalmazásáról és megállapításáról, WP 253, elfogadás időpontja: 2017. október 3.

Magas védelmi szint biztosítása a tagállamokban – az adatvédelmi bírság intézménye a védelmi lépcső fényében

Az uniós jogalkotó az egyes tagállamokban biztosított védelmi szintet eltérőnek látta, és ezt arra vezette vissza, hogy a Rendelet által hatályon kívül helyezett 95/46/EK adatvédelmi irányelv tagállami átültetése és gyakorlata országonként eltérő volt.[331] Annak érdekében, hogy a személyek magas szintű védelme szavatolható legyen, az érintetti jogokat az egész Európai Unióban azonos szintű védelemben kell részesíteni, a széttagolt szabályozást tehát fel kell számolni. Ennek eszköze és garanciája, hogy a „szabályok betartásának ellenőrzéséhez és biztosításához egyenértékű hatáskört is biztosítani szükséges, és a jogsértőkre azonos szankciókat kell kiszabni".[332] A Rendelet közvetlenül alkalmazandó jogalkotási aktusként ennek a jogalkotói szándéknak a keretét teremti meg. Minden korrekciós intézkedés a jogellenes adatkezelést eredményező jogviszonyba való közvetlen beavatkozást jelent, amely az adatok védelmét szolgálja. Ezen intézkedéseknek speciális és generális célja is van.

A védelmi lépcső elmélete tekintettel van mennyiségi és minőségi változásokra is. A bírság kiszabásának Rendeletben meghatározott szabályai markáns változást hoznak a Rendeletet megelőző időszakhoz képest. A jogalkotó a tagállamok jelentős részében már jelen lévő és alkalmazott jogintézményt honosított meg uniós szinten. Ez egy olyan vívmányként tartandó számon, amely tekintettel van a magánszférát érintő kockázatok jelenlétére, és a magánszférát súlyosan érintő jogsértések esetére az adatkezelő szervezet pénzügyi helyzetét is megfelelőképp befolyásolni képes eszközt ad a hatóságok kezébe.

A jogalkotó számol azzal, hogy a személyes adatok kezelése üzleti lehetőségeket rejt, ennek megfelelően a piaci verseny adatvédelmi szabályait megszegő szereplőkkel szemben az adatok üzleti értékét is figyelembe vevő intézkedést kínál. Ha a védelmi lépcső minimális elvárásait vesszük számba, akkor például a jogalkotó reális helyzetértékelése említendő. Itt pedig ezt érjük tetten. A védelmi lépcsőn az előrelépés jellemzője, hogy az adatkezelőket az adatkezelés kapcsán terhelő kötelezettségek az alkal-

[331] A Rendelet (9) preambulumbekezdésében az irányelv tagállami átültetésének éles jogalkotói kritikáját olvashatjuk.

[332] A Rendelet (11) preambulumbekezdésének utolsó mondata szerint.

mazott technológia és az üzleti modellek fényében fejlődnek. A hatóságok a bírság révén értékelni tudják az új üzleti megoldásokat, azok hatását a magánszférára.

> A bírság egy markáns, esetről esetre érvényesíthető beavatkozás az állam részéről. Következetesebb és igazságosabb megoldást kínálhat egy olyan közteher bevezetése, amely a személyes adatok kezelése után fizetendő. Elképzelésem szerint ez egy termékdíjként lenne bevezethető, amely lehetővé tenné, hogy a felhasználók által megosztott adatok révén szerzett profitot is igazságosan ossza meg az adatkezelő szervezet és a közösség. Vagyis itt egyfajta adóról lenne szó, amelynek a rendeltetése eltér a bírságétól. Nem váltaná, nem válthatja ki a bírságot, a két intézmény egymás mellett létezhetne.[333]

A bírság uniós szintű rögzítését a védelmi lépcsőn mindezek alapján előrelépésként értékelhetjük, hozzá kell egyszersmind azonban azt is tenni, hogy az egységesítés fájó hiányossága volt a Rendeletet megelőző időszaknak.

A pénzügyi szankció révén a védelmi lépcső minőségi indikátorai közül több is kedvező eredményt mutat. Az érintett jogai ugyan nem bővülnek ezáltal automatikusan, mégis, a jogérvényesítésre közvetetten bizonyosan hatással van. Az érintett az a személy, akivel az adatkezelő konfliktusa eljárási keretek között szankcióhoz vezethet. Az adatok alanya nem képes a pénzügyi szankciót kikényszeríteni, de az általa észlelt jogsértés esetén abba a helyzetbe kerül, hogy képes a szankcióhoz vezető eljárást megindítani. Közvetetten tehát a jogérvényesítés esélyei javulnak.

Szintén javulnak annak esélyei, hogy a jog hatékonyabban érvényesül. Az adatkezelő oldalán megjelenő pénzügyi kockázatok egyértelmű ösztönzői a jogi megfelelésnek. Ennek azonban már mennyiségi oldala is van, ennek megfelelően a kis összegű bírság nem jár a hatékonyság javulásának reményével. Az arányos, hatékony és visszatartó erejű szankció jár csupán minőségi javulással. A bírság mértéke kapcsán lentebb elemezni fogom azt, hogy a Rendelet szabályai megfelelnek-e ennek az elvárásnak.

A bírság mint védelmi komponens statikumában is értékelendő. Említettünk már olyan szabályozási elemeket, amelyek léte már önmagában is jelentős a védelem struktúrájában. Azzal, hogy a bírság az uniós jogban

[333] Vö. Szabó Endre Győző: Személyes adat kezelése után fizetendő termékdíj – avagy osszuk meg a megosztott adatok hasznát! *Pázmány Law Working Papers,* (2014), 29.

meghonosodott, gyakorlatilag nélkülözhetetlen része lett a védelmi rendszernek. A bírság intézménye sok dinamikus részletszabályt rejt, ugyanakkor arra is rá kell mutatni, hogy a védelmi lépcsőben a bevezetés puszta ténye is minőségi javulásként mutatható ki.

A bírság kiszabásának mérlegelése

A Rendelet részletes kritériumrendszert határoz meg annak mérlegelésére, hogy szükség van-e bírság kiszabására, a bírság összegének megállapítására. Ez a két mérlegelés azonos szempontok alapján történik, a jogalkotó nem hozott létre két eltérő szempontrendszert.[334] A hatóság tehát ugyanazokat a körülményeket vizsgálja akkor, amikor arról dönt, hogy kiszabjon-e bírságot, és akkor is, amikor a bírság mértékéről határoz. Az alábbiakban áttekintem ezt a kritériumrendszert a magyar és a nemzetközi gyakorlat fényében, konkrét eseteket is feldolgozva. A hatóságok bírságolási gyakorlata nem csupán gyakorlati szempontból jelentős, hanem a védelem szintjének meghatározása terén is iránymutató jellegű-e: a jogsértéseknek azt a fokát jelöli, ahol a hatóságok a legsúlyosabb korrekciós hatáskörükkel élnek, és pénzügyi szankciót alkalmaznak.

A bírság kiszabásának szempontjai és a védelmi lépcső alkalmazása

A mérlegelés szempontjait a védelmi lépcső fényében a következőképpen elemzem: nem térek ki minden kritérium kapcsán arra, hogy milyen módon járul hozzá a rendeleti szabályozás előttihez képest a védelem erősítéséhez, ugyanakkor, ahol ez releváns, megemlítem azokat az előrelépési lehetőségeket, amelyek összességében a védelem következő szintjének megfelelő javulást képesek megteremteni. Nem állítom azt, hogy egy-egy javasolt részletszabályozási elem önmagában előrelépést jelentene a védelmi lépcsőn. Azzal a céllal értekezem a védelem szintjének emeléséről, hogy az a védelmi lépcső következő fokában beépülhessen a szabályozási elemek közé, és ilyen módon szolgálja a magánszféra erősebb védelmét. Amennyiben arra jutok, hogy a szabályozás ezen a téren nem fejlesztendő, úgy ilyen tartalmú következtetést fogalmazok meg.

[334] A Rendelet 83. cikk (2) bekezdésében a felsorolást bevezető mondat szerint.

A jogsértés jellege, súlyossága, időtartama

A mérlegelés során az anyagi jogi jogsértés jellegét, súlyosságát és időtartamát vizsgálja a hatóság, továbbá vizsgálja az érintettek számát és az általuk elszenvedett kár mértékét. A jogsértés jellege és súlya döntő befolyást gyakorol a bírság mértékének meghatározására, hiszen – amint azt a bírság mértéke kapcsán be fogom mutatni – a Rendelet egyes rendelkezéseinek megsértése enyhébbnek, illetve súlyosabbnak minősülhet, és ez az alkalmazandó szankcióra is hatással van.

A Rendelet „kisebb megsértése" esetén[335] a bírság kiszabása helyett az elmarasztalás alkalmazását teszi lehetővé. Ebben az esetben a hatóságnak különös figyelmet kell fordítania a jogsértés természetére, súlyosságára, időtartamára, továbbá a kötet további részében elemzendő szempontokra. A „kisebb megsértés" esetén végső soron egy kivételszabályról van szó, nem a Rendelet szabályainak mellőzéséről, hanem a Rendelet hatékony alkalmazásával összeegyeztethető esetről, amikor az enyhítő körülmények kombinációja a bírság kiszabásának mellőzéséhez vezet.

Az az időtartam, ameddig a jogsértés fennáll, szintén mérlegelési szempont. E tekintetben az is figyelembe veendő, hogy mennyire lett volna kézenfekvő a jogsértő helyzet megszüntetése, vagy éppen a kockázat enyhítése.[336]

A hatósági mérlegelés tárgyát képezi az is, hogy a jogsértés egyedi, ügyintézői mulasztásra vezethető vissza, vagy rendszerszintű problémára utal. Az ügyintézői mulasztás vagy akár figyelmetlenség enyhébben ítélendő meg, mint a rendszerszintű problémák jelenléte. Különösen nagyobb, jelentős személyi állományú szervezetek esetében az elvárások is magasabbak ezen a téren.[337]

[335] Lásd a Rendelet (148) preambulumbekezdésének második mondatát.

[336] A NAIH/2020/1160. sz. ügyben a hatóság figyelembe vette a később incidenshez vezető adatbiztonsági rés könnyű és ingyenes javíthatóságát, amelyet az adatkezelő elmulasztott megtenni. Szintén súlyosító körülményként értékelte, hogy az adatkezelő a saját belső szabályozását sem tartotta be, amikor a hiba elhárítását elmulasztotta.

[337] A NAIH mérlegelte ezt a szempontot a NAIH/2018/6142-es, továbbá a NAIH/2019/2471-es és a NAIH/2019/2485-ös számú ügyekben hozott határozataiban. A NAIH/2020/1160-as számú ügyben a NAIH azt is mérlegelte, hogy az ügyféltől a piaci pozíciója alapján fokozottan elvárható a megfelelő adatbiztonsági intézkedések alkalmazása.

E pontot illetően nem fogalmazok meg konkrét szabályozási javaslatot. Az itt mérlegelt szempontok szoros összefüggést mutatnak az elszámoltathatóság elvének szervezeten belüli érvényesítésével, ami pedig az adatvédelmi kultúra erősítése révén javítható. Az adatvédelmi tisztviselő sikeres munkájának eredményeként ebben a tekintetben is fejleszthető a szervezet eredményessége.

A kár mértéke

Az érintettek által elszenvedett kár mértéke szintén mérlegelési szempont. Itt többféle kár jöhet számításba, így természetesen a pénzben kifejezhető vagyoni vagy fizikai kár, de a magánszféra körében értékelhető valamennyi kár és kockázat is mérlegelendő. A természetes személyek jogait és szabadságait érintő kockázatok között említi a Rendelet például a személyazonosságlopást vagy a személyazonossággal való visszaélést.[338] A bírság természetesen nem a kár megtérítésére irányul, hiszen itt egy szankcióról van szó, a kár minél pontosabb meghatározása mindazonáltal hozzátartozik a bírságkiszabás gondos mérlegeléséhez.

Amennyiben a jogellenes adatkezelés az érintettre nézve súlyos következménnyel jár, indokolhatja a bírság kiszabását. A következmény lehet gazdasági, szociális vagy mindkettő együtt. Ezekben az esetekben a figyelmeztetés alkalmazása nem lenne megfelelő jogkövetkezmény.[339]

Az előrelépés lehetősége a védelmi lépcsőn

Előrelépést jelentene álláspontom szerint, ha a kár mértékéig vagy a megszerzett vagyoni előny erejéig is kiszabható lenne a bírság. Nem fogadható

[338] Lásd a Rendelet (75) preambulumbekezdését, amely részletes leírást ad a természetes személyek jogait és szabadságait érintő, a személyes adatok kezeléséből származó kockázatokról. A kockázatokat és a magánszféra kapcsolatát fentebb részletesen elemeztem.

[339] A NAIH 2019/596-os számú ügyben a Kecskemét Megyei Jogú Város Önkormányzata által létrehozott költségvetési szerv adatkezelése ügyében folytatott eljárás keretében jutott erre a következtetésre. A közalkalmazott jogviszonyának megszüntetése, amihez a jogellenes adatkezelés vezetett, természetesen jelentős következményként értékelendő.

el ugyanis, hogy az adatok jogellenes kezelése révén, a szankció jogalkotó által meghatározott mértékének korlátai miatt gazdagodhasson a jogsértő. Kétségtelen, hogy e ponton felmerül a bizonyíthatóság, nevezetesen az, hogy a kár mértékének megállapítása adott esetben szakértői kérdés. Ez a lehetséges gyakorlati nehézség nem változtat azon az elérendő célon, amely a szankcionálás mértékét nem a jogalkotói számokhoz, hanem a jogellenes magatartással elért vagy elérni kívánt nyereséghez igazítja. Amellett érvelek, hogy az adatkezelő maga kell hogy mérlegelje: ha a jogellenes magatartás jelentős hasznot ígér, azonos mértékben jelenik meg a szankció végösszege is a kalkulációban.

Tisztában vagyok a kikényszeríthetőség és a bizonyíthatóság korlátaival, ezért itt is utalok az adatvédelmi tisztviselő által betölthető új szerepre, amely szerint az új adatkezelések esetén a tisztviselő jóváhagyását kell igényelni. Ennek hiányában az új adatkezelést bejelentik, így a hatóság tudomást szerez a tervezett műveletről. Ilyen módon garantálható, hogy az adatkezelések ne maradjanak látenciában, a láthatatlan adatokon végzett műveletek láthatóvá váljanak a hatóságok számára.

A kár enyhítése érdekében tett intézkedések

A kár enyhítése érdekében tett intézkedés enyhítő körülmény a bírság kiszabásának megfontolásakor, illetve mértékének meghatározásakor. Itt minden olyan intézkedés szerepet játszhat, amely végső soron az adatalanyokat érintő, az adott adatkezeléssel összefüggő károk enyhítéséhez hozzájárulhat.[340] Harmadik fél, más adatkezelők értesítése a további károk megelőzésében vagy enyhítésében, vagy a saját szervezeten belül olyan intézkedések meghozatala, amelyek a súlyosabb következményeknek elejét veszik – ezek mind jelentős mértékben figyelembe vehetők enyhítő körülményként.

[340] A Rendelet (148) preambulumbekezdése szerint a bírságösszeg megállapítása során kellő figyelmet kell fordítani többek között arra, hogy „tettek-e intézkedéseket az elszenvedett kár mértékének csökkentésére".

Az előző pontban amellett érveltem, hogy a szankció mértékét a kár mértékéhez kell igazítani. Amennyiben ezt kimondjuk, úgy a kár enyhítése érdekében tett lépések értéke is mérendő, és figyelembe veendő a bírság konkrét összegének kalkulációja során. Ez a szabály hozzájárulhat ahhoz is, hogy az adatkezelők magasabb tudatosság mellett lássák el tevékenységüket. Egy ilyen szabály léte önmagában is ösztönzést jelent az adatkezelő szervezetek számára, hogy az adatok kezelését illetően a költségeket felmérjék, és a magánszférát érintő hatások a szervezet üzleti terveiben valós értéken jelenjenek meg. Az ilyen szabályozás azzal jár, hogy láthatóbbá válik a magánszféra értéke, az adatok kezelését érintő, ködbe vesző körülmények kalkulálhatóvá válnak.

Az érintettek száma

Az érintettek számának meghatározása a tényállás feltárásának egyik fontos eleme. Utal egyrészt a jogsértés következményeinek súlyosságára, másrészt pedig az érintettek számából arra is következtetni lehet, hogy egyszeri jogsértés történt, vagyis ügyintézői hiba folyományáról, vagy rendszerszintű jogsértésről van szó. Amennyiben elszigetelt eseményről van szó, az értelemszerűen kisebb súllyal esik latba az adatkezelői felelősség mérlegelése során, és erősítheti azt a feltételezést, hogy az adatkezelő szándéka nem terjedt ki a jogsértés elkövetésére.

A magyar bírói gyakorlat az érintettek számának meghatározását illetően nem teljesen következetes. A Fővárosi Közigazgatási és Munkaügyi Bíróság a 29.K.34.567/2015/16. számú ítéletében döntő jelentőségűnek találta, hogy a két vizsgált adatkezelő által folytatott adatkezelést el lehessen különíteni, ehhez pedig szükség lett volna az adatalanyok számának pontos meghatározására. Ugyanaz a bíróság egy másik ügyben (13.K.32.819/2015/16.) a jelentős számú érintett esetében nem tartotta szükségesnek a hatósági határozat e megállapítását precízen alátámasztani, mert az adatkezelői nyilatkozat, amely szerint „fél Magyarországnyi" adatot kezelnek, nem hagy kétséget afelől, hogy a megállapítás megalapozott. A Fővárosi Törvényszék a 2.K.31.506/2018/8. számú ügyben szintén úgy foglalt állást, hogy a jelentős számú adatalany érintettsége

nyilvánvaló, az érintetti kör pontos meghatározása pedig „nem matematikai kérdés", ha egyébként a nagyságrendhez nem fűződik kétség.

Felmerül a kérdés, hogy az egyetlen adatalanyt érintő jogellenes adatkezelés lehet-e olyan súlyú, ami a bírság kiszabását indokolhatja. A tipikusan az érintetti joggyakorlás körébe tartozó esetekben a gyakorlat megerősíti, hogy egyetlen érintett esetében is vezethet az eljárás adatvédelmi bírság kiszabásához.[341]

Az előrelépés lehetősége a védelmi lépcsőn

Lehetséges jövőbeni szabályként javasolható, hogy az érintettek száma tekintetében ne csupán a ténylegesen megvalósult jogsértéseket vegye figyelembe a jogalkalmazó, hanem mindazon személyeket is vegyék számba, akiknek a magánszférájára a jogellenes adatkezelési szándék irányult. A jogsértés tehát ne csupán eredményszempontból, hanem szándék szerint is essen értékelés alá. Ez a kitétel ismét bizonyítási kérdéseket vet fel, mindazonáltal bizonyíthatóság esetén nem látom okát annak, hogy miért maradhatna szankcionálatlanul a magánszféra megsértésére irányuló szándék. Ez a kérdés természetszerűleg kapcsolódik a lentebb tárgyalandó szándékosság, illetve gondatlanság problematikájához.

A jogsértés szándékos vagy gondatlan jellege

A jogsértés szándékos vagy gondatlan jellegének megítélése során figyelembe kell venni a jogsértő ismeretét és szándékát az adott jogsértés kontextusában. A szándékosság meglétét erősíti, ha a jogsértés hosszabb időn keresztül valósul meg. Szintén szándékosságra utal, ha a jogellenesség a felső vezetés tudtával, jóváhagyásával vagy például az adatvédelmi tisztviselő állásfoglalásával kifejezetten szembehelyezkedve történik. Hasonlóan

[341] A NAIH számos esetben szabott ki bírságot olyan ügyekben, amikor csupán egyetlen érintett, az ügy kérelmezője esetében állapított meg jogsértést. Így például a NAIH/2018/6093-as, a NAIH/2018/7235-ös, a NAIH/2018/7142-es, a NAIH/2019/1859-es számú ügyekben csupán egy érintett adatainak kezelését vizsgálta.

ítélendő meg, ha az adatvédelmi felügyeleti hatóság korábbi iránymutatásával összeegyeztethetetlen az adatkezelés.[342]

Amennyiben a belső szabályzatok értelmezésének bizonytalansága, egyszeri emberi hiba, frissítések elmulasztása áll a jogsértés hátterében, ez a gondatlanság megállapítását valószínűsíti.[343] A gondatlan elkövetés kellő körültekintéssel elkerülhető lenne. Az ilyen esetekben a szándékosság a körülmények vizsgálata alapján kizárható.

Amennyiben a szándékosság megállapítható, az az adatvédelmi bírság összegének kiszabásakor értelemszerűen a magasabb irányba mutat. A hatóságok esetjogában ritkább a szándékosság megállapítása, azt a körülmények alapján a hatóság köteles bizonyítani.

Az előrelépés lehetősége a védelmi lépcsőn

A szándékosság kapcsán itt is utalok az adatvédelmi tisztviselő lehetséges jövőbeni szerepére. Bár a Rendelet alkalmazásának jelenlegi formájában is kiemelhető a tisztviselő funkciója, a jövőbeni szerep, amint azt a tisztviselőről szóló fejezetben kifejtem, még kevesebb kétséget hagy a szándékosság vagy gondatlanság megítélésében.

A felelősség mértéke

A felelősség mértéke szintén kötelezően mérlegelendő szempont. Mind az adatkezelő, mind az adatfeldolgozó kötelezettsége, hogy az érintettek jogait fenyegető kockázatokkal arányosan, az adatbiztonság, a beépített és az alapértelmezett adatvédelem elveivel összhangban megfelelő technikai és szervezési intézkedéseket hajtson végre.[344] Ez az adatkezelés összetett-

[342] A NAIH/2019/55-ös számú ügyben a fesztivál szervezőjének adatkezelését vizsgálva jutott arra a következtetésre a magyar hatóság, hogy bizonyos adatok kezeléséről a hatóság már megállapította azok szükségtelen voltát, az adatkezelő mégis ragaszkodott a hatóság által helytelennek talált gyakorlathoz.

[343] Lásd az európai adatvédelmi testület iránymutatását, 12.

[344] A NAIH határozatait vizsgálva arra is következtethetünk, hogy bizonyos adatkezelőkkel szemben a felelősség mértéke körében figyelembe veszi például a piaci pozícióját. A piacon nagy szereppel bíró adatkezelőkkel szemben a jogszabályoknak való megfelelés terén az elvárások is fokozottak (pl. a NAIH/2020/1160. sz. ügy).

ségétől függően bonyolult belső szabályozást és intézkedések együttesét követelheti meg. E körben az adatkezelő nem hivatkozhat például erőforráshiányra, hiszen a Rendelet által követett kockázatarányos megközelítéssel ez nem lenne összeegyeztethető.

Az adatvédelmi bírság egy szankció, amelynek alkalmazása során vizsgálandó a felróhatóság. Az adatkezelő felróhatósága megállapítható kell hogy legyen, ha az adatkezelői magatartás révén az érintett nem tudja jogait gyakorolni. Ha az érintettet megfosztják a joggyakorlás lehetőségétől, az a bírság kiszabása mellett szól.[345]

Korábbi releváns jogsértések

A korábban elkövetett releváns jogsértések értelemszerűen jelentős szerepet játszanak a jogsértés súlyosságának megítélésében. A Rendeletet megelőző magyar szabályozásban a kis és közepes méretű vállalkozások esetében az első jogsértést nem is lehetett bírsággal szankcionálni, ehelyett figyelmeztetést kellett alkalmazni.[346] Ez a szabály a Rendelet alkalmazandóvá válásával elveszítette jelentőségét az adatvédelem területén, mindenesetre ez is utal a visszaesés fontosságára. A Rendelet nem bármely, hanem csak a „releváns" jogsértésre utal, ennek megfelelően az ugyanolyan típusú vagy az azonos módon elkövetett jogsértés játszik szerepet. A testület iránymutatása szerint ilyen eset lehet, ha például az érintetti kérelmek nem megfelelő kezelése miatt azonos módon több jogsértés fordul elő úgy, hogy a korábban elkövetett jogsértést szankció követte.[347]

Korábbi hatósági intézkedések ugyanabban a tárgyban

Az előbbihez hasonló, de külön szempont az, ha az adatkezelővel szemben korábban elrendelték a hatóság korrekciós hatáskörébe tartozó valamelyik intézkedést ugyanabban a tárgyban. Az előző pontban a releváns jogsértés,

[345] A NAIH egy konkrét esetben alkalmazta ezt a mérlegelési szempontot, a NAIH/2018/6093-as számú ügyben.

[346] A kis- és középvállalkozásokról, fejlődésük támogatásáról szóló 2004. évi XXXIV. törvény rendelkezett erről a mentességről.

[347] Lásd az európai adatvédelmi testületi iránymutatást, 15.

e pontban pedig az ugyanabban a tárgyban született hatósági intézkedés az elemzés tárgya. A releváns jogsértés nem csupán hatósági eljárást követően, hanem például bírósági határozatban is megállapítható, ennek megfelelően az előbbi tágabb, míg az utóbbi szűkebb körben veendő figyelembe, azzal, hogy a második súlyosabb megítélés alá eshet, hiszen már legalább két alkalommal vizsgálja ugyanazt a jogsértést a hatóság, és ennek ellenére sem küszöbölték ki a jogellenességet.

Az előrelépés lehetősége a védelmi lépcsőn

Az ugyanabban a tárgyban a korábbi hatósági intézkedések mérlegelése a bírság megállapítása során egy statikus védelmi komponens, ahogyan az előzőekben tárgyalt felelősség és felróhatóság mértékének figyelembevétele, valamint a korábbi releváns jogsértések mérlegelése. Továbbfejlesztésükre nincs szükség és mód, megőrzésük azonban a magas védelmi szint fenntartása érdekében szükséges.

A tudomásszerzés módja

Az is vizsgálandó, hogy a felügyeleti hatóság milyen módon szerzett tudomást a jogsértésről, különösen, ha azt az adatkezelő maga jelentette be a hatóságnak. A Rendelet az adatvédelmi incidensek kötelező bejelentését írja elő. Ha a hatóság a jogsértésről így szerez tudomást, úgy az nem tartozik abba a körbe, amikor a bejelentés az adatkezelő javára lenne írható, hiszen csupán jogszabályi kötelezettségét teljesítette. Bár az adatvédelmi incidens fogalma tágan is értelmezhető, a jogsértések széles körében fordulhat elő, hogy incidens ugyan nem történt, mégis, a jogsértés feltárása és következményeinek enyhítése érdekében hasznos lehet a hatóság értesítése. A Rendelet ebben a körben ezeket az eseteket szabályozza és kedvezőbb jogkövetkezményt fűz hozzájuk.

> A Rendelet 4. cikk 12. pontja szerint adatvédelmi incidens a biztonság olyan sérülése, amely a továbbított, tárolt vagy más módon kezelt személyes adatok véletlen vagy jogellenes megsemmisítését, elvesztését, megváltoztatását, jogosulatlan közlését vagy az azokhoz való jogosulatlan hozzáférést eredményezi.

Az incidensek késedelmes bejelentése vagy a bejelentés elmulasztása egyértelműen súlyosbító körülmény a bírság kiszabásának mérlegelése során. Az incidensbejelentés kötelezettségével egy olyan jogintézmény honosodott meg az Európai Unióban, amelynek célja az adatkezelő szervezeteken belüli és azon kívüli transzparencia erősítése, az érintettek jogainak és érdekeinek védelme.

A késedelmes vagy elmaradó bejelentés mindezeket az érdekeket sérti, és az adatkezelői oldalon megvalósuló mulasztás azért is esik jelentős súllyal a latba, mert sok esetben az adatkezelő az egyetlen szereplő, aki fel tudja mérni az incidens lehetséges következményeit.

Az is előfordulhat, hogy még az adatkezelő sem képes a következmények felmérésére, megbecsülésére, és éppen ezekre az esetekre jelent garanciát az adatvédelmi hatóság bevonása, amely a kockázatok értékelése alapján elrendelheti az érintettek kötelező tájékoztatását.

Ez utóbbi esetben az adatkezelő felelőssége fokozott, de természetesen az első esetben is egyértelmű. Az incidens bejelentésének elmulasztása gyakorlatilag egy védelmi intézkedés kijátszását jelenti, ami jelentős érv a szankció alkalmazása mellett. Az adatkezelő szervezetén belül az incidens észlelése utáni intézkedések életbe léptetése helyes eljárás, de nem teszi meg nem történtté a hatóság tájékoztatásának elmulasztását, amit önálló jogsértésként kell számon tartani.

A NAIH több esetben is megállapította az adatkezelő felelősségét az incidens bejelentésének elmulasztása miatt.
A NAIH/2019/2668-as számú ügyben nem csupán a bejelentés elmulasztását, hanem azokat az azonnali intézkedéseket is figyelembe vette a hatóság, amelyeket az incidens kiváltó okának megszüntetése érdekében tettek. Az előbbit jelentős súlyosbító, az utóbbit enyhítő körülményként mérlegelték.
A NAIH/2019/3854-es számú ügyben szintén a bejelentés elmulasztása miatt szabott ki bírságot a hatóság. Kifogásolta, hogy „az incidens kezelésének […] hiányában az incidensnek […] tényleges kockázatai sem mérhetők fel kellőképpen, ami önmagában is kockázatot jelent".
A NAIH/2019/2471-es számú ügyben a hatóság az említett esetek tényállásán túl azt is kifogásolta, hogy az adatkezelő a saját belső eljárásrendjét is figyelmen kívül hagyta. Nemcsak hogy nem értesítették a hatóságot 72 órán belül, de a tudomásszerzést követően is csak 27 nappal később végezték el a kockázatelemzést. Ez az adatkezelői eljárás is adatvédelmi bírságot eredményezett.

Az előrelépés lehetősége a védelmi lépcsőn

A tudomásszerzés módjának mérlegelése a bírság megállapítása során egy természetében statikus védelmi komponens, tartalma azonban bővíthető, és bővítendő is. A védelmi lépcsőn való előrelépés egyik szemléletbeli váltása az, hogy a hatósággal szembeni transzparencia logikája megfordul: nem az számít enyhítő körülménynek, ha a hatóságot az adatkezelő egy jogsértőnek tűnő gyakorlatról tájékoztatja, hanem az számít súlyosbító körülménynek, ha ezt elmulasztja megtenni. Itt utalok a jog hatékonysága kapcsán tett észrevételekre, különösen Barfuss gondolataira, aki szerint a nem hatékony normák egyik típusa az olyan jogszabály, amelynek végrehajtása komolyan nem ellenőrizhető. Márpedig a személyes adatok védelmére vonatkozó jogszabályok kifejezetten e kategóriába tartoznak akkor, ha nem egészítjük ki erős garanciális követelményekkel őket. Ezt a célt szolgálja a transzparenciaszabályok megfordítása, és az adatkezelő szervezetek átláthatóságának erősítése. A magánszférát érintő tevékenységek ugyanis a nehezen követhető technológiákkal megvalósítva kikövetelik a védelmet szolgáló kompenzációt.

A jogsértéssel érintett adatkategóriák

A jogsértés által érintett adatkategóriák kitétele tulajdonképpen a Rendelet fogalommeghatározására utal. A 9. cikk határozza meg a személyes adatok különleges kategóriáit, idetartozik többek között az egészségügyi adat, a szexuális életre vagy szexuális irányultságra vonatkozó adat, továbbá a genetikai és biometrikus adat.

> A Rendelet 9. cikke szerint az adatok különleges kategóriáit a következők képezik: a faji vagy etnikai származásra, politikai véleményre, vallási vagy világnézeti meggyőződésre vagy szakszervezeti tagságra utaló személyes adatok, valamint a természetes személyek egyedi azonosítását célzó genetikai és biometrikus adatok, az egészségügyi adatok és a természetes személyek szexuális életére vagy szexuális irányultságára vonatkozó személyes adatok.

A 10. cikk a büntetőjogi felelősség megállapítására vonatkozó határozatokra, valamint a bűncselekményekre vonatkozó személyes adatokra utal.

Az Infotv. által korábban alkalmazott különleges és bűnügyi személyes adat fogalmához hasonló felosztást alkalmaz a Rendelet, azzal a fontos különbséggel, hogy a genetikai és biometrikus adatok a különleges adatkategóriák közé kerültek.

A személyes adatok említett kategóriái világos jogszabályi definíción alapulnak. A védelem megfelelő szintjének garantálása érdekében azonban nem szabad figyelmen kívül hagyni az érintett helyzetét, ilyenkor figyelemmel kell lenni az ő személyes életét potenciálisan fenyegető kockázatokra. A személyes adatok védelmére vonatkozó szabályozás szívében nem csupán formális jogi kérdések állnak, hanem annak érdemi vizsgálata, hogy a jogellenesség eredményeként előállt helyzet miképpen befolyásolja az érintett társadalmi helyzetét, magánszféráját, szűkebb és tágabb értelemben egyaránt. A szakmai feladatok végrehajtásához köthető információk is lehetnek adott esetben érzékenyek, vagy egy sajátos vagy éppen kiszolgáltatott élethelyzet szintén vezethet olyan eredményhez, amelyben az adatok ugyan nem minősülnek a definíció szerint különleges adatkategóriába tartozónak, a jogalkalmazásnak azonban mégis reagálnia kell a fokozott védelmi igényre.

A NAIH/2019/2471-es számú ügyben egy rendőri szervnél dolgozók adatait érintő incidens kapcsán mutatott rá a hatóság indokolásában, hogy az adatok „jogosulatlan megismerése jelentős következményekkel járhat az érintettek számára […]; ilyen adatok kezelésekor az adatkezelőknek fokozott elővigyázatossággal kell eljárniuk."
A NAIH/2019/3854-es számú ügyben a magyar hatóság a „kiszolgáltatott élethelyzetben lévő, kiskorú" személyek adatait érintő incidensben jelentős mértékben vette figyelembe e körülményt a bírság szükségességének mérlegelésekor.

A Rendelet alapján adott esetben releváns lehet, hogy az adatok lehetővé teszik-e a személyek azonosítását, vagy éppen álnevesített adatállományról van szó. Anonim adatok esetében a Rendelet nem alkalmazandó, hiszen az érintettek nem azonosíthatók, és ilyen módon a magánszféra sérelme nem valósul meg. Az álnevesített adatok esetében az mérlegelendő, hogy az adatok közvetetten ugyan, de azonosíthatók maradnak, ezért az álnevesített adatok személyes adatként kezelendők, még akkor is, ha egyébként a jogsértés révén az érintettek valószínűsíthetően nem váltak azonosíthatóvá.

A Rendelet (26) preambulumbekezdésének második mondata szerint „[a]z álnevesített személyes adatok, amelyeket további információ felhasználásával valamely természetes személlyel kapcsolatba lehet hozni, azonosítható természetes személyre vonatkozó adatnak kell tekinteni".

A jogsértést az álnevesítés nem teszi meg nem történtté, a személyes adatok védelmének sérelme megállapítható, mindazonáltal az álnevesítés a kár mértéke, illetve a kár enyhítésének érdekében tett intézkedések körében enyhítő körülményként értékelhető.

Az előrelépés lehetősége a védelmi lépcsőn

A jogsértéssel érintett adatkategóriák, valamint az érintett helyzetének vizsgálata a bírság kiszabásának mérlegelése kapcsán egy statikus szabályozási komponens, dinamikus tartalommal. Ez a dinamizmus nemcsak ügytípusonként, hanem ügyenként is érvényesül, ezzel pedig valóban eljutunk az adatvédelmi gyakorlat mikroszintjére. Az elemzés ilyen mélysége kimondottan szándéka is a védelmi lépcsőről való gondolkodásnak.

Az egyén helyzetének vizsgálata minden adatvédelmi szabályozás sajátja, a védelmi lépcsőn történő előrelépés esetén ezt a szempontot szintén érvényesíteni kell.

A magatartási kódex és a tanúsítás szerepe a bírságkiszabás során

Az adatkezelő az adatvédelemre vonatkozó szabályoknak való megfelelést magatartási kódex alkalmazásával vagy tanúsítás révén is igazolhatja. A bírság mérlegelése során a hatóság vizsgálja, hogy az adatkezelő tartotta-e magát a jóváhagyott magatartási kódexhez vagy a tanúsítási mechanizmushoz. Bár a hatóság nincsen kötve az ilyen önszabályozási eszközök keretében alkalmazott jogkövetkezményekhez, adott esetben megelégedhet a magatartási kódex ellenőrző szervének intézkedésével, és a hatóság ilyenkor nem alkalmaz szankciót.[348] A kódex alkalmazásának felfüggesztését vagy a kódex alkalmazásából való kizárás lehetőségét a hatóság értékelheti hatékony, arányos és visszatartó erejű szankciónak.

[348] Lásd európai adatvédelmi testületi iránymutatás, 16.

A tárgyalt szempontok közül a magatartási kódex és a tanúsítás szerepét tartom a legkevésbé kidolgozottnak, ebből következően pedig ebben lehet a legkevésbé előremutató megállapításokra jutni. A Rendelet mögött húzódó jogalkotói cél nagy szerepet szán az adatkezelői önszabályozásnak. Különös módon azonban az adatkezelők meglehetősen szerény eredményeket értek el ezen a téren a Rendelet alkalmazásának első éveiben. Az önszabályozás az adatvédelmi szabályozásnak egy fontos alkotóeleme, hosszabb távon is kívánatos a jelenléte, az eddigi gyakorlat azonban óvatosságra int a hosszabb távú következtetések levonásában. Mindennek alapján a kívánatos jövőbeni szabályozás, a következő szint megállapítása terén nem teszek megállapításokat.

Egyéb körülmények

Egyéb súlyosbító vagy enyhítő körülmények említésével zárul a Rendelet 83. cikkének kritériumrendszere. Ez csupán egy példálózó felsorolás, amelyben a jogsértés következtében szerzett pénzügyi haszon vagy elkerült veszteség szerepel. A hatóság ezeken túl természetesen minden olyan szempontot figyelembe vehet, amely az ügy megítélésében szerepet játszik. A megszerzett vagyoni előny például fontos érv lehet a szándékosság megállapítása körében, valamint nyomós érv a bírság kiszabása mellett.

A hatóságok mindenképpen figyelembe veszik az adatkezelő szervezet együttműködésének fokát. A felügyeleti hatósággal való együttműködés mértéke akkor releváns, ha a jogsértés orvoslásához és a jogsértés negatív hatásainak enyhítéséhez hozzájárul. Egyébként a hatósággal való együttműködés önmagában nem minősül enyhítő körülménynek.[349] Az, hogy az együttműködésből adódóan milyen intézkedések vezettek adott esetben a jogsértés orvoslásához, illetve hatásainak enyhítéséhez, esetről esetre ítélhető csak meg.

[349] A Rendelet 31. cikke alapján az adatkezelő és az adatfeldolgozó a felügyeleti hatósággal – annak megkeresése alapján – együttműködik. A tárgyalt esetben ezen túlmutató, kezdeményező jellegű együttműködésre van szükség ahhoz, hogy enyhítő körülményként legyen figyelembe vehető.

Az adatkezelő magatartása az érintett védelmére akkor is hatással van, ha éppen hatósági eljárás van folyamatban. Ennek megfelelően nem közömbös, hogy az adatkezelő szervezet ebben az időszakban, az eljárás idején milyen mértékben működik együtt a hatósággal. Az együttműködést illetően három fokozatot különböztethetünk meg egymástól. A védelem szempontjából a legkedvezőbb eset az, amikor az adatkezelő szervezet olyan mértékben működik együtt a hatósággal, amely túlmutat a jogszabályok által elvárt szinten, és ezt a hatóság enyhítő körülményként tudja figyelembe venni. (A NAIH/2019/55-ös számú ügyben a hatóság enyhítő körülményként vette figyelembe, hogy a „Kötelezett a hatóság korábbi felszólításának részben eleget tett", és ennek eredményeként már az eljárás alatt módosította az egyébként összetett adatkezelési folyamatát.) A második vagy középső szintje az együttműködésnek az, amikor az adatkezelő szervezet minden kötelezettségét pontosan teljesíti, azonban ez nem jár olyan többlettel, amelyet a hatóság figyelembe vehetne mint enyhítő körülményt. (A NAIH/2019/596-os számú ügyben a hatóság ugyan elismerte az adatkezelő oldalán az együttműködési szándékot, „noha e magatartást – mivel a jogszabályi kötelezettségek betartásán nem ment túl – kifejezetten enyhítő körülményként nem értékelte". Hasonlóan értékelte az adatkezelő eljárását a NAIH/2018/5457-es számú ügyben is.) Az érintettek védelmét tekintve a legkedvezőtlenebb szintet akként határozhatjuk meg, hogy ilyen esetben az adatkezelő még a jogszabályban elvártakat sem teljesíti, tehát a minimum alatti fokon áll az együttműködési hajlandóság. Ilyenkor a hatóságnak az adatkezelő ilyen jellegű mulasztását érvényesíteni kell a szankciókban. Ez a magatartás álláspontom szerint önmagában is indokolttá teszi az adatvédelmi bírság kiszabását, de mindenképpen figyelembe veendő a bírság összegének meghatározásakor.

A NAIH/2019/167-es számú ügyben az adatkezelő először az érintettet, majd a hatóságot is tévesen tájékoztatta az adatkezelés körülményeiről. Csupán a hatóság ismételt felszólítására adott tájékoztatást arról, hogy az érintett mely adatait kezeli. A hatóság eljárása során akként értékelte az adatkezelő együttműködését, hogy az „nem az elvárható mértékben működött együtt a hatósággal a jogsértés kivizsgálása és orvoslása érdekében".

A NAIH/2019/1598-as számú ügyben a hatóság figyelembe vette, hogy az általa kibocsátott végzésre az adatkezelő nem nyújtott megfelelő tájékoztatást, ezáltal nehezítette a tényállás feltárását, és „további eljárási cselekmény foganatosítását tette szükségessé".

A hatósággal való együttműködés mellett azt is számon kell tartani, hogy milyen módon törekszik az adatkezelő arra, hogy az előállt jogellenes helyzetben igyekezzen a személyes adatok védelmét előmozdítani. Ez az adatkezelői erőfeszítés megkülönböztetendő az imént tárgyalt, hatósággal való együttműködéstől. Az előbbi elsősorban a tényállás feltárását, a transzparenciát szolgálja, utóbbi pedig az adatkezelés érdemi körülményeinek javítására irányul.

A NAIH/2019/2472-es számú ügyben a hatóság enyhítő körülményként értékelte, hogy az adatkezelő még a hatósági eljárás megindítása előtt intézkedéseket tett arra, hogy az általa jogszerűtlenül továbbított adatok címzettjei töröljék a birtokukba jutott személyes adatokat.
Hasonlóan kedvezően értékelte a hatóság az adatkezelő intézkedését a NAIH/2019/2466-os számú ügyben, amikor még az eljárás ideje alatt módosította adatvédelmi tájékoztatóját, ilyen módon a jogszerű körülmények megteremtése érdekében soron kívül intézkedéseket tett.

Figyelembe vehető szempont még az is, ha az érintett maga is közrehat a jogellenes állapot előidézésében, illetve magatartásával ő maga is megnehezíti annak megoldását.

Az előrelépés lehetősége a védelmi lépcsőn

Amint az az előzőekből kiolvasható, a személyes adatok kezelésének technológiai és piaci feltételeit alapul véve jelentős változtatásokat tartok szükségesnek ahhoz, hogy a védelmi lépcsőn valóban minőségi előrelépés történjen. Ez a szemléletváltás érinti a hatósággal való együttműködést is. Álláspontom szerint a hatóságok új és erős pozíciója elképzelhetetlen az adatkezelőknél rendelkezésre álló információkhoz való zökkenőmentes hozzáférés nélkül, anélkül, hogy az adatkezelők együttműködnének a hatósággal. A fent tárgyalt együttműködési fokozatokat ennek megfelelően módosítani kell, és a legmagasabb fokú együttműködést kell neutrálisnak tekinteni, minden egyéb esetben az együttműködés elégtelen, és a szankció megállapítása során ennek megfelelően kell figyelembe venni.

A bírsággal szemben támasztott általános elvárások

Közigazgatási bírságot „A felügyeleti hatóságok hatásköre" című fejezetben tárgyalt korrekciós hatáskörét gyakorolva a tagállami adatvédelmi felügyeleti hatóság szab ki. Ennek három esetét szabályozza a Rendelet:

- enyhébb megítélés alá eső anyagi jogi jogsértések;
- súlyosabban értékelendő anyagi jogi jogsértések és
- a hatóság utasításának be nem tartása.[350]

Mindegyik esetben csak a bírságtétel legmagasabb összege szabályozott, ez alatt a hatóság széles körű mérlegelés alapján szab ki bírságot. A kiszabott bírságnak az ügy összes körülményének mérlegelése alapján hatékonynak, arányosnak és visszatartó erejűnek kell lennie.

A magyar hatóság a bírsághatározatok indokolásában ezt a kritériumot is figyelembe veszi, így például a NAIH/2019/596-os számú határozatában úgy fogalmazott, hogy szerepét „csak akkor képes a jogkövetkezmény, jelen esetben a bírság betölteni, ha a Kötelezett számára érezhető mértékű, és általában is hasonló kötelezettek számára visszatartó hatása lehet".
Egy másik határozatban szintén az „érezhető mértékű" fordulatot használja a NAIH (NAIH/2019/55), megint egy másikban a „legalábbis érzékelhető nagyságú" fordulatot (NAIH/2019/2471), végül pedig a „nem jelent teljesíthetetlen kötelezettséget, ugyanakkor érezhető mértékű" érvelést használja (NAIH/2019/2076).

Ez a követelmény magában foglalja azt az elvárást is, hogy minden ügyet egyedi mérlegelés alapján kell megvizsgálni, általános bírságtételek nem alkalmazhatók. Mivel bírságtételeket ugyan nem alkalmaznak a hatóságok, azzal próbálkoznak, hogy egyfajta bírságképlet vagy -táblázat alapján tegyék kiszámíthatóbbá és egységesebbé a bírságok kiszabásának gyakorlatát.

Az arányosság követelménye egyedi mérlegelést követel meg. Ha a közigazgatási bírságokat vállalkozásoktól eltérő személyekre szabják ki, a felügyeleti hatóságnak figyelembe kell vennie a jövedelmek általános szintjét

[350] A Rendelet 58. cikk (2) bekezdésében meghatározott korrekciós intézkedésekre utal a jogalkotó.

az adott tagállamban, valamint az adott személy gazdasági helyzetét.[351] Különös jelentősége van ennek természetes személyek esetében.

> Tekintettel arra, hogy a bírságnak nincsen alsó határa, a természetes személyek esetében is van lehetőség jelzésértékű, alacsony mértékű bírság kiszabására. Ennek jogrendszerbeli szerepe az elmarasztalás és a bírság között helyezhető el.

A hatékonyság-arányosság-visszatartó erejű hármas kritérium kapcsán azt is mérlegelni kell, hogy mi a bírság célja: az adatkezelő terelése a jogszerű magatartás irányába, avagy – különösen súlyosabb és szándékos jogsértés esetén – az adatkezelő és az adatkezelő magatartásának büntetése. A Rendelet szabályozási koncepciójával mind a két cél összhangban áll.

A bírság mértéke

A Rendelet által bevezetett bírságösszeg a hatáskörökre vonatkozó szabályozással együtt egységesen érvényesül az Európai Unióban, ez pedig újdonság. A tagállamok joga, ahol erre vonatkozó szabály érvényesült, országonként eltérő összegű bírságmaximumokat állapított meg. A korábbi széttagoltság ezen a téren is megszűnt. Az új bírságösszegek a korábbi tagállami szabályozáshoz képest jelentősen megemelkedtek.

Enyhébb megítélésű jogsértések

Az enyhébb megítélésű anyagi jogi jogsértések esetén legfeljebb 10 millió euró összegű bírság, a vállalkozások esetében pedig az előző pénzügyi év teljes éves világpiaci forgalmának legfeljebb 2%-át kitevő összegű bírság szabható ki. A kettő közül a magasabbat kell alapul venni.

Az enyhébbnek minősülő esetek közé tartozik:

– a gyermek hozzájárulásával összefüggő jogsértés az információs társadalommal összefüggő szolgáltatások körében,[352]

[351] A Rendelet (150) preambulumbekezdése szerint.
[352] A Rendelet 8. cikkében foglalt követelmények alapján.

– az érintett azonosítását nem igénylő adatkezelésre vonatkozó szabályok megsértése,[353]
– az adatkezelő és az adatfeldolgozó kötelezettségeire vonatkozó általános szabályok megsértése,

Az adatkezelőt és az adatfeldolgozót széles körben terhelő kötelezettségek tartoznak ide, így a beépített és az alapértelmezett adatvédelem követelménye, a közös adatkezelőkkel szembeni elvárások, az unióban tevékenységi hellyel nem rendelkező adatkezelők képviselőire vonatkozó előírások, az adatfeldolgozóra vonatkozó szabályok, az adatkezelési tevékenységek nyilvántartása, a felügyeleti hatósággal való együttműködés kötelezettsége, az adatkezelés biztonsága kapcsán az általános elvárások, az adatvédelmi incidens bejelentésének kötelezettsége, az érintett tájékoztatásának kötelezettsége az adatvédelmi incidensről, az adatvédelmi hatásvizsgálat és az ennek kapcsán kezdeményezendő előzetes konzultáció, az adatvédelmi tisztviselő kijelölésére, jogállására és feladataira vonatkozó szabályok. Szintén ebbe a körbe tartozik még a tanúsításra és a tanúsítószervezetekre vonatkozó szabályozás.

– a tanúsítószervezetre vonatkozó szabályok megsértése,[354]
– továbbá a magatartási kódexnek való megfelelést ellenőrző szervezet mulasztása, amikor egy adatkezelővel szemben a kódex alkalmazása felfüggesztésének vagy a kódex alkalmazásából való kizárásnak lenne helye.[355]

Az utolsó két pont az önszabályozás, illetve az önkéntes alapú tanúsítás esetén nyitva hagyja a hatóságok szankcionálási lehetőségét annak érdekében, hogy ne válhasson az ilyen szabályozás alatt zajló adatkezelés ellenőrizhetetlenné, illetve ne lehessen ezeket kivonni a bírságfenyegetettség alól.

[353] A Rendelet 11. cikkében írt szabályok alapján.
[354] A Rendelet 42. és 43. cikke szerint.
[355] A kódexnek való megfelelés ellenőrzését végző szerv e kötelezettségét a Rendelet 41. cikkének (4) bekezdése írja elő.

Súlyosabb jogsértések

A súlyosabban értékelendő anyagi jogi jogsértések esetén legfeljebb 20 millió euró összegű bírság, a vállalkozások esetében pedig az előző pénzügyi év teljes éves világpiaci forgalmának legfeljebb 4%-át kitevő összegű bírság szabható ki. A kettő közül a magasabbat kell alapul venni.

A súlyosabban minősülő esetek közé tartozik:

- az adatkezelés elveinek megsértése,[356]
- a hozzájárulás megadásának, illetve beszerzésének szabályait érintő jogsértés, az érintettek jogait sértő adatkezelés,[357]
- személyes adatok harmadik országbeli címzett részére történő jogellenes továbbítása,[358]
- az adatkezelés különös eseteire vonatkozó tagállami rendelkezések megsértése.[359]

Ezeken túl szintén ebbe a kategóriába tartozik a felügyeleti hatóság olyan utasításának be nem tartása, amellyel az adatkezelést átmenetileg vagy véglegesen korlátozza, vagy az adatáramlást felfüggeszti.

Az adatvédelmi felügyeleti hatóság vizsgálati hatáskörében eljárva, több más jogosultság mellett, feladatai ellátása céljából tájékoztatást kérhet az adatkezelőtől, adatvédelmi auditot végez, hozzáférést kap a feladatellá-

[356] A Rendelet 5., 6., 7. és 9. cikkében szabályozott elvek, így a jogszerűség, tisztességes eljárás és az átláthatóság a célhoz kötöttség, az adattakarékosság, a pontosság, a korlátozott tárolhatóság, az integritás és bizalmas jelleg, valamint az elszámoltathatóság elve. Az adatkezelés jogszerűségére (jogalapjára) vonatkozó szabályok, kiemelten is a hozzájárulás feltételei és a személyes adatok különleges adatkategóriáira vonatkozó szigorúbb szabályok tartoznak ebben a körben a Rendelet elvei közé.

[357] A Rendelet 12–22. cikkei szerint az érintettnek nyújtandó tájékoztatásra, az adatokhoz való hozzáférésre, a helyesbítéshez, törléshez (az elfeledtetéshez), az adatkezelés korlátozásához, az adathordozhatósághoz, a tiltakozáshoz való jogra vonatkozó szabályok. Itt említendő még az egyedi ügyben történő automatizált döntéshozatal a profilalkotással együtt – az érintetti jogok védelme ezekre az esetekre is kiterjed.

[358] A Rendelet 44–49. cikkei szabályozzák a harmadik országba irányuló adattovábbítás feltételeit.

[359] A Rendelet IX. fejezete szerint a tagállamok sajátos követelményeiket bizonyos területeken összeegyeztethetik a személyes adatok védelméhez fűződő jog érvényesülésére irányuló általános szabályokkal. A szabályozási tárgykörök: a véleménynyilvánítás szabadsága és a tájékozódáshoz való jog; a személyes adatok kezelése és a hivatalos dokumentumokhoz való nyilvános hozzáférés; a nemzeti azonosító számok kezelése; a foglalkoztatással összefüggő adatkezelés.

tásához szükséges valamennyi személyes adathoz és információhoz, hozzáférést kap az adatkezelő bármely helyiségéhez, ideértve minden felszerelést és eszközt. Amennyiben ez a hozzáférési jog sérül, úgy az adatkezelővel szemben szintén a magasabb bírságtétel alkalmazásának van helye. Azért is figyelemre méltó ez az utóbbi bírságtétel, mert ez gyakorlatilag egy eljárási szankció.

A Rendelet az anyagi jogi mellett eljárási kérdéseket is szabályoz, így különösen a tagállami felügyeleti hatóságok közötti együttműködést és a testület működését. A bírságokat mindig egy-egy tagállami adatvédelmi felügyeleti hatóság szabja ki önálló mérlegelése alapján, akkor is, amikor a határon átnyúló ügyben hatóságok közötti együttműködési eljárás zajlik. A tagállami hatóságok az adott tagállami közigazgatási eljárási szabályok szerint járnak el a Rendelet alkalmazása során. Az anyagi jogi szempontrendszer egységes, de a tagállami alkalmazás továbbra is harmonizálatlan közigazgatási eljárási rendben történik. A különbözőségekből adódhatnak olyan esetek, amikor például az egyik tagállamban közigazgatási értelemben már elévült ügyben nem indítható eljárás, míg a másik tagállam esetében az ügy még nem évült el.

Itt nem anyagi jogsértésről van szó, hanem az adatvédelmi felügyeleti hatóság vizsgálati hatáskörének akadályozásáról. Ez az eljárási jellegű szabály a Rendeletben rögzített kevés, de hasznos előírás közé tartozik. Amellett, hogy az ilyen magas bírságfenyegetettség kedvezően hathat a hatósággal való együttműködési hajlandóságra, egy apró lépés az EU szintjén egységesedő és rendkívül kívánatos eljárási szabályozás irányába.

A felügyeleti hatóság utasításának figyelmen kívül hagyása

A felügyeleti hatóság utasításának be nem tartása esetén az előbb említett magasabb bírságösszeget kell alapul venni, a két összeg közül ebben az esetben is a magasabbat kell alkalmazni.

A bírság legalacsonyabb és legmagasabb összege

A kiszabható bírságnak nincsen minimális összege, így tehát jelképes összegű, akár egyeurós bírság is kiszabható.

A magyar szabályozás 2012-től tette lehetővé a NAIH számára a bírság kiszabását, a bírságösszeg minimumát az Infotv. 100 ezer forintban határozta meg. Jelképes összegű bírság kiszabására tehát nem volt lehetőség, ami hiányossága volt a magyar szabályozásnak. Az Infotv. a költségvetési szervekre alkalmazható bírságtételek körében megtartotta a 100 ezer forintos minimumbírságösszeget. Ez utóbbi megoldás már azért illethető kevesebb kritikával, mivel itt nem magánszemélyekről, hanem költségvetési szervezetekről van szó, ahol a megélhetési kérdések nem játszanak közvetlen szerepet.

Több jogsértés esetén, amikor az alacsonyabb és a magasabb bírságösszeggel fenyegetett magatartás is megvalósul, akkor a magasabb bírságküszöb alkalmazandó, annál magasabb bírságösszeg kiszabására nincs lehetőség. E téren sem a gondatlan, sem a szándékos elkövetés nem befolyásolja a bírságszámítás módját.[360]

Az előrelépés lehetősége a védelmi lépcsőn a bírság összege terén

A bírság intézménye, ahogyan arra fentebb utaltam, fontos építőeleme a védelem rendszerének. A bírság lehetséges maximális összege korántsem mennyiségi kérdés, hanem tudatos választás kérdése: a jogalkotó eleget tesz-e annak az általános uniós elvárásnak, hogy a szankció valóban arányos, hatékony és elrettentő erejű legyen. Álláspontom szerint a százalékos és a meghatározott összegű bírságtétel alkalmazása fontos előrelépés a korábbi uniós szabályozáshoz képest. Előrelépést jelent a harmonizált szabályok alkalmazása az EU-ban, hatékonyabb jogérvényesítést, erősebb tudatosságot eredményez a jogalkalmazásban. A Rendelet szabályai a védelmi lépcső fényében világos előrelépést jelentenek a Rendeletet megelőző időszakhoz képest.

A védelmi lépcső következő szintjéhez tartozó kedvezőbb szabályozás a Rendeletben alkalmazott bírságtételeken túl lehetővé teszi az okozott kárhoz vagy az elért anyagi előnyhöz igazodó bírságok alkalmazását is, ahogyan erről már szóltam. Enélkül a bírságok legmagasabb összege nem minden esetben igazodik a valósághoz. A bírságok terén érvényesülő jogalkotói kompromisszum a Rendeletet a védelem alacsonyabb szintjén tartotta. Egyértelmű hiányosságként kell számontartanunk, hogy a bírság nem

[360] A Rendelet 83. cikk (3) bekezdése alapján.

a valós károkhoz, hanem egy elméleti számítás kereteihez igazodik. Nem azt állítom, hogy a Rendeletben alkalmazott bírságösszegek alacsonyak, hanem azt, hogy nem az elérhető legmagasabb szintű fenyegetést, és az ezzel járó védelmet nyújtják a magánszféra szempontjából.

Kivel szemben szabható ki bírság?

A korábbi szabályozáshoz képest újat hoz a Rendelet annyiban, hogy a bírságot nemcsak az adatkezelőre vagy az adatfeldolgozóra lehet kiszabni, hanem a magatartási kódex alkalmazását ellenőrző szervezetre és a tanúsítószervezetre is. A Rendeletnek való megfelelés, illetve ennek számonkérése terén a két utóbbi szervezetnek is van szerepe és felelőssége. A Rendelet tehát azt a szabályozási koncepciót követi, hogy ahova felelősséget telepít a jogszabálynak való megfelelés érdekében, ott ezt kiegészíti a szankciókkal való fenyegetettséggel, ideértve a közigazgatási bírságot is.

Adatkezelő bárki, így nemcsak egy vállalkozás, közfeladatot ellátó szerv, hanem természetes személy is lehet, ebből következően konkrét esetben a bírság címzettje természetes személy. Az ő esetükben a Rendelet alapján kiszabható bírságösszegek nyilvánvalóan aránytalanul magasak, ezért a Rendelet kifejezetten megengedi, hogy velük szemben bírság helyett elmarasztalást alkalmazzon a hatóság. Egyébként is figyelembe vehető az adott ország jövedelmi helyzete, kerülendő az aránytalan bírságok alkalmazását.

A bírság összegének meghatározása kapcsán láttuk, hogy vállalkozások esetén az éves világpiaci forgalom 2, illetve 4%-áig terjedő plafon érvényesül. A vonatkozó preambulumbekezdés szerint a vállalkozás fogalmát a bírságösszeg meghatározása céljából az Európai Unió működéséről szóló szerződés 101. és 102. cikkében meghatározott vállalkozásokra vonatkozó szabályoknak megfelelően kell értelmezni, a Rendelet (150) preambulumbekezdésének harmadik mondata szerint. Az Európai Unió Bíróságának gyakorlata szerint a vállalkozás fogalma minden gazdasági tevékenységet folytató jogalanyra kiterjed, függetlenül annak jogállásától és finanszírozási módjától.[361] A vállalkozás fogalma alatt olyan gazdasági egység is értendő, amely egy anyavállalatból és leányvállalatokból áll,

[361] C-41/90. sz. Klaus Höfner és Fritz Elser versus Macrotron GmbH ügyben 1991. április 23-án hozott ítélet (EBHT 1991., 1979. o.) 21. pontja.

továbbá vállalkozásnak tekintendő az a gazdasági egység, amely kereskedelmi, illetve gazdasági tevékenységet folytat, függetlenül az érintett jogi személytől.[362]

A bírsággal sújtható személyi kör meghatározása – az előrelépés lehetősége a védelmi lépcsőn

A Rendeletet megelőző időszakban bizonyos szereplők bírságolása nem volt lehetséges, vagy legalábbis nem volt elvárás uniós szinten. Végső soron a tagállami jogalkotóra bízták, hogy milyen személyi körben teszi alkalmazhatóvá a pénzügyi szankciót. Amint láttuk, számos ország nem is ismerte ezt a jogkövetkezményt. A Rendelet ennek megfelelően olyan hiányt pótolt, ami a védelem szempontjából jelentős mulasztásnak tekinthető. A védelem igényét a jogalkotó minden olyan jogellenesség szankcionálásával jelzi, ahol az adatok kezelését befolyásoló döntések születnek. A döntés és a teljes adatvédelmi jogi felelősség tehát összekapcsolódik, a felelősség pedig a szankcionálást is magában foglalja.

A Rendelethez képest előrelépést jelentene bizonyos magatartások szankcionálása. Azokban az esetekben, amikor az adatvédelmi tisztviselőt nem tájékoztatják az új, tervezett adatkezelésről, ez a tájékoztatási mulasztás is szankcionálandó álláspontom szerint. A transzparencia elvárása a minőségi előrelépés érdekében elengedhetetlen. Ez egy adatkezelő szervezeten belüli mulasztás, mégis, a tisztviselő új szerepét számításba véve a tájékoztatás elmulasztása súlyos transzparenciadeficitként értékelendő.

Szintén szankcionálandó magatartásként tartandó számon az az eshetőség, ha maga az adatvédelmi tisztviselő nem tesz bejelentést az adatvédelmi hatóságnak az olyan adatkezelésről, amellyel kapcsolatban kifogást fogalmazott meg. Ebben az esetben az adatvédelmi tisztviselőt is szankcióval kell fenyegetni, mert ő maga szeg meg egy átláthatósági, elszámoltathatósági szabályt. Azért is fontos a külső szankció lehetősége, mert a tisztviselőre adott esetben nehezedhet belső nyomás, hogy egy tervezett adatkezelést támogasson. Ennek a nyomásnak az ellensúlyozására hatékony eszköz lehet a hatósági szankció. Nem feltétlenül csupán pénzügyi szankciót tartok alkalmasnak. A tisztviselőt, az általam ideálisnak tartott szabályozás keretei között, egyfajta kamarai tagsági kötelezettség is terheli. E kamara

[362] Az európai adatvédelmi testületi iránymutatás, 6.

keretei között is alkalmazható szankció, például a tagság felfüggesztése vagy egyéb fegyelmi eszközök. A védelem szintjének minőségi javítása érdekében a tisztviselő szerepe tehát itt is jelentős.

Közhatalmi szervek bírságolása

A 29-es munkacsoport *Iránymutatás az adatvédelmi tisztviselőkkel kapcsolatban*[363] című dokumentuma foglalkozott a „közhatalmi szerv vagy egyéb, közfeladatot ellátó személy" fogalmával. A dokumentumban az Európai Unió adatvédelmi hatóságai úgy foglaltak állást, hogy ezt a fogalmat, illetve személyi kört a tagállami jogban kell meghatározni. Ennek megfelelően uniós definíciója ebben az összefüggésben nem létezik.

Az általános adatvédelmi Rendelet alkalmazandó minden olyan adatkezelésre, amely az uniós jog alapján nem esik kívül a hatályán. Ahogyan Váradi Szilvia rámutat, a közszférában működő szervezetek nagy számban gyűjtenek és tárolnak személyes adatokat, amelyek közül sok kifejezetten szenzitívnek is minősül.[364] Ennek megfelelően a Rendelet szabályozásának kiterjesztése a közszférára magától értetődően adódik. Tagállami szinten alkalmazásának körét szűkíteni tehát nem lehet. Ez alól az általános elv alól kivétel a bírságkiszabás szabályozása, ugyanis a Rendelet ezen a téren kifejezetten lehetővé teszi a tagállami szabályozást. A vonatkozó preambulumbekezdés szerint a „tagállamokra kell bízni annak eldöntését, hogy a közhatalmi szervekkel szemben alkalmazható legyen-e közigazgatási bírság, és ha igen, milyen mértékű".[365] Ennek megfelelően a tagállami jogalkotó dönthetett arról, hogy kíván-e a saját adatvédelmi felügyeleti hatóságának olyan hatáskört biztosítani, amely a közhatalmi szervek bírságolását is magában foglalja. Három szabályozási modell lehetséges:

– a jogalkotó olyan jogszabályt alkot, amely a Rendelet bírságokra vonatkozó szabályait mindenkire nézve, így a közhatalmi szervekre is alkalmazandónak rendeli;

[363] WP 243 rev.01

[364] Váradi Szilvia: A közszférára vonatkozó adatvédelmi szabályok a GDPR tükrében. *Pro Futuro,* 9. (2019), 1. 39–54.

[365] A Rendelet (150) preambulumbekezdésének utolsó előtti mondata szerint.

– a jogalkotó olyan jogszabályt alkot, amely a közhatalmi szervek esetében is lehetővé teszi a bírság alkalmazását, de számukra egy „kedvezőbb" rezsimet vezet be;
– a jogalkotó nem teszi lehetővé a közhatalmi szervek bírságolását.

Nem a Rendelet alkalmazása alóli általános mentesülésről van szó, csupán arról, hogy jogsértés esetén a közhatalmi szervek kivételszabály alá tartoznak, és őket közigazgatási bírsággal nem lehet sújtani. A közhatalmi szervek bírságolása elleni érvként szokás említeni, hogy a kiszabott bírságösszeg az államháztartáson belül marad, legfeljebb az egyik alrendszerből átkerül a másik alrendszerbe, büntetés jellege ilyen módon nem érvényesül. A bírságolás mellett említhető az a megfontolás, hogy akár közhatalmi, akár magánszektorba tartozó adatkezelőről legyen is szó, ugyanazon személyek magánszférája érintett, a védelem tárgya ugyanaz, ez pedig az azonos elbírálás irányába mutat.

A bírságolás hatályát illetően a jogalkotásért felelős szerveknek gyakorlati és jogpolitikai megfontolások alapján kellett e kérdésekben dönteniük. Az Infotv. vonatkozó rendelkezése szerint amennyiben a hatóság a Rendelet fentiekben elemzett 83. cikke alapján szab ki bírságot, és a bírság megfizetésére kötelezett „költségvetési szerv", úgy a bírság mértéke 100 ezer forinttól húszmillió forintig terjed.[366] A bemutatott elvekkel összhangban a magyar Országgyűlés úgy döntött, hogy a bírsággal való fenyegetettséget a közszféra körében is fenntartja. Ezzel a hatáskörével a magyar adatvédelmi hatóság egyébként következetesen él is.

Ez a modell érvényesül az Európai Adatvédelmi Biztos (EDPS) esetében is, amely az Európai Unió intézményeinek felügyeleti szerveként hatáskörrel rendelkezik bírság kiszabására. Az EDPS a működésére vonatkozó Rendelet 66. cikke szerint alkalmanként legfeljebb 25, illetve súlyosabb esetben 50 ezer eurós bírságot szabhat ki. A bírság összege éves keretben is maximált. A részletes szabályokat az Európai Parlament és a Tanács (EU) 2018/1725 rendelete (2018. október 23.) a természetes személyeknek a személyes adatok uniós intézmények, szervek,

[366] Az Infotv. 61. § (4) bekezdése rendelkezik a bírságtételről. A jogalkotó ezzel gyakorlatilag a korábbi bírságtételeket hagyta hatályban. A Rendelet elemzéséhez szorosan nem kapcsolódik ugyan, de az Infotv. szerint a magyar hatóság a bűnüldözési, nemzetbiztonsági és honvédelmi célú adatkezelések esetében is lehetővé teszi a pénzügyi szankció alkalmazását.

hivatalok és ügynökségek általi kezelése tekintetében való védelméről és az ilyen adatok szabad áramlásáról, valamint a 45/2001/EK Rendelet és az 1247/2002/EK határozat hatályon kívül helyezéséről tartalmazza.

Az előrelépés lehetősége a védelmi lépcsőn

A közhatalmat gyakorló szervek bírságolása nem csupán mennyiségi kérdés. Nem arról van csak szó, hogy hány adatkezelőre összesen mekkora összegű bírságot lehet kiszabni, vagy ténylegesen mennyit szab aztán ki az adatvédelmi hatóság. A bírság összege a védelem minőségi kérdése, hiszen a bírsággal való fenyegetettség a kiszabható bírságmaximummal arányos ösztönzőt jelent. Ez további bizonyítást nem igénylő ténykérdés. Az is kétségtelen, hogy a közhatalmat gyakorló szervek esetében nem mindig lehetséges az „árbevétel" mérése, hiszen az sok szervezet vonatkozásában egyszerűen értelmezhetetlen. Ezt nem tekinthetjük jelentős jogértelmezési problémának, hiszen a Rendelet eleve vagylagosan határozza meg a bírságmaximumot.

Két irányt tartok lehetségesnek a védelem erősítése érdekében.

Az egyik lehetséges szabálymódosítás kiterjesztené a kiszabható bírságösszegeket a közhatalmi szervekre, minden tagállami különbségtétel nélkül. Nem a tagállami implementáló szabályokat, hanem magát a Rendeletet kellene módosítani ennek érdekében. A jelenlegi szabályozás egy jelentős tagállami eltérésre ad lehetőséget, amelynek alapján azt állapíthatjuk meg, hogy a GDPR ugyan rendeleti formát öltött, de ezen a ponton irányelvi jellegű szabályt állapít meg.

A másik a személyes felelősség megjelenítése. Az adatkezelő szervezet felső vezetőjét jogszabálysértés esetén természetesen különböző eljárásokban felelősségre lehet vonni. Ennek számos formája létezik. A személyes adatok védelmének erősítése érdekében megfontolandónak tartjuk egy ilyen felelősségi szabály bevezetését. Akár az általános munkajogi szabályokra való utalás is elégséges lehet, amelyek a felelősség kérdését minden tagállamban rendezik. Az utaló szabály meghatározhatná, hogy minden olyan esetben, amikor a felső vezető mulasztása kimutatható,[367] akkor a munka-

[367] Elképzelhetők olyan esetek is, amikor a legnagyobb körültekintés mellett is megvalósul a jogsértés, tipikusan egyéni, jogellenes magatartás révén. Az ilyen esetekben a felső vezető személyes felelősségének megállapítása nemkívánatos.

jog szabályai szerinti korlátok között helytállni tartozik a szervezetet ért kárért. A kár ebben az esetben megjelenhet adatvédelmi bírság, kártérítés, sérelemdíj, de akár nem vagyoni, például reputációs kár formájában is. Ahogyan a tisztviselő szerepe kapcsán utaltam arra, hogy a feladat ellátása nem válhat személytelenné, úgy az ilyen szabály is erősítené a szervezet vezetőjének személyes felelősségét.

Egységes bírságolási gyakorlat az unió tagállamaiban a védelmi lépcső fényében

Fentebb szóltam már a védelmi szintről, és ennek kapcsán a hatáskörök egységesítéséről, a szankciók szigorításáról, továbbá a Rendelet betartatásának erősítéséről. Mindennek alapja, hogy a Rendelet, ideértve a bírságra vonatkozó szabályokat is, egységes módon érvényesüljön minden tagállamban. A határon átnyúló ügyekben a hatóságoknak együtt kell működniük, ennek során van lehetőség véleményüket kifejteni az adott üggyel kapcsolatban. Azokban a helyi ügyekben, amelyek adott esetben anyagi jogi értelemben azonosak akár a más tagállamban előforduló helyi ügyekkel, akár együttműködési eljárásban vizsgált más ügyekkel, szintén törekedni kell a harmonizációra szerte az Európai Unióban. A tagállami eltérések kiküszöbölése nélkül nem valósulna meg a védelem szintjének egyenszilárdságára irányuló jogalkotói cél. Erre az egységes gyakorlatra törekszenek a tagállami adatvédelmi hatóságok. A közös megközelítés egyik eredménye az az iránymutatás, amelyet ebben az elemzésben is feldolgozok.

E kérdés kapcsán nem tartom alkalmazhatónak a védelmi lépcső elméletét tiszta formájában, mert a 95/46/EK adatvédelmi irányelv időszakában, tehát a Rendeletet megelőzően nem is létezett az a jogalkotói cél, hogy a bírságok kiszabása terén egységes gyakorlat érvényesüljön. Ennek megfelelően a rendeleti szabályozás olyan újdonságot jelenít meg ezzel az elvárással, ahol csak a jelenlegi fokot tudjuk azonosítani, valamint a következőt, ahova a védelmi lépcsőn kívánatos lenne továbblépni.

A Rendelet alkalmazását végigkíséri az a küzdelem, amelyet a *forum shopping* ellen folytatnak a tagállamok. A legkedvezőbb fórum megtalálása attól függetlenül jelen van az adatkezelő szervezetek gyakorlatában, hogy erről a jogalkotó vagy a hatóságok tudomást vesznek-e. Az egységes bírságolási gyakorlat kialakítása kapcsán rá kell mutatni arra, hogy sikertelenség

esetén egy lefelé irányuló tendencia lesz megfigyelhető. Az adatkezelők szívesebben telepednek majd le olyan tagállamokban, ahol az adatkezelőkkel szembeni bírságolás gyakorlata kedvezőbb. Ilyen módon nemcsak a *forum shopping* jelenségével szembesülünk, hanem a védelem eróziójával is. Amennyiben ugyanis a Rendeletben meghatározott bírságtételeket a gyakorlat alakítja, esetenként „lefelé húzza", úgy meghiúsul az a jogalkotói szándék, amely szerint az unió magas védelmi szintet kíván biztosítani. Ez a jogalkotói szándék nem valósul meg, ha a tagállamok közötti egyenetlenségek révén alacsonyabb és magasabb szintű védelem egyszerre van jelen, a jogi szabályozás pedig nem tudja hathatósan megakadályozni a kedvezőbb fórum megválasztását.

Az előrelépés lehetőségét itt nem jogalkotásban, még csak nem is a hatáskörök további koncentrációjában látom. Az előrelépés itt egy kiterjedt és türelmes munka eredményeként születhet meg, amelynek révén a hatóságok a hasonló ügyekben hasonló szankciókat alkalmaznak. Az egységességnek az a foka, amit a „hasonló" helyett az „azonos" jelzőkkel tudnánk leírni, valószínűleg csak a laboratóriumban létezik, ebben reálisan kell látnunk. Az egységességnek létezik azonban egy elérhető szintje, amely a fennálló kisebb különbségek mellett sem csábítja az adatkezelőket a leírt taktikai megfontolások szerint a másik tagállamba való letelepedésre. Bár a védelmi lépcsőn a „fordított gravitáció" jelenségét is meghatároztam, e ponton azt kell kimondani, hogy a hatóságok szoros és összehangolt tevékenysége nélkül csak a lefelé mutató irányba fog a gyakorlat elmozdulni. Tény, hogy a széttöredezettség egyelőre létező jelenség, de az Európai Adatvédelmi Testületen belül a bírságolással kapcsolatos tevékenységeket ellátó szakértői alcsoport remélhetőleg sikeres munkát végez majd ezen a téren is, és a védelmi lépcsőn való előrelépést eredményező egységesítés valósul meg a következő időszakban.

A Rendelet eddigi gyakorlata alapján azt látjuk, hogy még nem született elegendő mennyiségű bírsághatározat ahhoz, hogy a gyakorlat egységességéről vagy annak hiányáról megalapozott következtetést vonhassunk le. Ugyanakkor az a tény, hogy számos tagállamban a Rendelet teremtette meg a bírság kiszabásának lehetőségét, és ennek gyakorlatát ezekben az országokban most alakítják ki, valószínűsíti, hogy egyelőre fennállhatnak olyan mértékű különbségek, amelyek az elemzés szempontjából jelentősek.

Együttműködési eljárások és vitarendezés, hatóságok függetlensége

Az elemzésben fentebb kitértem a felügyeleti hatóságok szerepére, továbbá elemeztem azt is, hogy a hatóságok új szemléletű feladatellátása milyen hatást gyakorolhat a védelem szintjére. Hiányos lenne az elemzés annak megvizsgálása nélkül, hogy milyen módon érinti a Rendelet által bevezetett új eljárásrend a hatóságok egymáshoz való viszonyát, különös tekintettel a közös hatáskörgyakorlásra és a függetlenségükre. Az alábbiakban kitérek az együttműködési eljárások egyes sajátosságaira, és áttekintem a hatóságok egymástól való függőségének és függetlenségének kérdéseit.

A jelenlegi szabályozás jellemzői – az együttműködés főbb szabályai – egyablakos ügyintézés és vitarendezés

Az egységes joggyakorlat kialakításának legközvetlenebb és leglátványosabb módja az úgynevezett egyablakos ügyintézés. A Rendelet 60. cikke szerinti eljárás határon átnyúló ügyekben folytatható, amikor a tevékenységi központ alapján illetékes fő felügyeleti hatóság *(lead supervisory authority)* döntéstervezetét a többi érintett hatóság *(concerned supervisory authority)* gyakorlatilag vétójog birtokában véleményezi.

> A Rendelet 4. cikk 22. pontja szerint érintett felügyeleti hatóság az, amelynek területén az adatkezelő tevékenységi hellyel rendelkezik, illetve a területén az adatkezelés jelentős mértékben érint vagy valószínűsíthetően érint adatalanyokat, továbbá az a hatóság is érintett hatóságnak tekintendő, amelyhez panaszt nyújtottak be az adatkezelés tárgyában.

Egyet nem értés esetén az érintett hatóság releváns és megalapozott kifogást nyújthat be a döntéstervezettel szemben, ami a bírságkiszabás kapcsán is megtehető, mert például hiányolja a bírságot vagy a mértékével nem ért egyet. Ha a hatóságok a kifogást követően egyhangúlag jóvá tudják hagyni az új határozattervezetet, úgy a fő felügyeleti hatóság a végleges határozatot kézbesíti az adatkezelőnek. Ebben az esetben az együttműködő hatóságok között konszenzus jön létre, és ilyen módon épül a közös esetjog, amelyet az egységes jogalkalmazás érdekében a helyi, határon át nem nyúló ügyekben is figyelembe kell venni.

A releváns és megalapozott kifogást követően a második, rövidebb határidővel sorra kerülő egyeztetés tétje, hogy a testület elé kerül-e az ügy. Amikor ugyanis a konszenzus nem jön létre, és a kifogást a vezető hatóság vagy a többi hatóság nem tudja elfogadni, illetve a kifogással összhangban álló, módosított tervezettel szemben más érintett hatóságtól érkezik kifogás, úgy az ügy a vitarendezési eljárás keretében a Testülethez kerül.[368]

A Rendelet a Testület feladatául szabja, hogy biztosítsa annak egységes alkalmazását, ennek érdekében ellenőrzi és biztosítja a Rendelet „helyes alkalmazását".[369] A testület ezt a szerepét részben a vitarendezési eljáráson keresztül tölti be. A vonatkozó preambulumbekezdés szerint „[a]z egységességi mechanizmus a közigazgatási bíróságok összehangolt alkalmazásának előmozdítására is felhasználható".[370] A testületnek arra is van lehetősége, hogy bizonyos kérdésekben véleményt bocsásson ki, vagy általános érvényű kérdésben foglaljon állást,[371] ezek a lehetőségek azonban nem kapcsolódnak szorosan egyes határozatokhoz, ezért itt nem szólok róluk bővebben, csupán a vitarendezési eljárást emelem ki.

Az eljárási szabályok különbözősége kapcsán meg kell említeni néhány olyan nehézséget, amelyek érintik a Rendelet egységes alkalmazását. Az uniós jogalkotó a Rendelet révén nem kívánta az eljárásjogokat harmonizálni, de utal az uniós jog és az Európai Unió Alapjogi chartájában rögzített elvekre, a megfelelő eljárási garanciákra, ideértve a hatékony jogvédelmet és a tisztességes eljáráshoz való jogot.[372] A Rendelet keretében egy olyan közös hatáskörgyakorlásra kerül sor a hatóságok együttműködésében, amely felszínre hozhat egymással nem kompatibilis szabályokat vagy gyakorlatokat. Az adatvédelmi hatóságok határozatait az esetleges jogorvoslat során az adott tagállami közigazgatási bíróság fogja megvizsgálni, a vizsgálat alapja pedig a tagállami közigazgatási eljárásjog. A Rendelet alkalmazása

[368] Az eljárás rendjét a Rendelet 60. és 65. cikke szabályozza.

[369] A Rendelet 70. cikk (1) bekezdésének a) pontja szerint.

[370] A Rendelet (150) preambulumbekezdése szerint.

[371] Ezen eljárások szabályait a Rendelet 64. cikkének (1) és (2) bekezdése szabályozza. Az (1) bekezdés szerinti eljárásrendben hagyta jóvá a testület például a hatásvizsgálati listákra vonatkozó tagállami hatósági döntéseket (így a magyar listát 10/2018-as számon). A (2) bekezdés szerinti eljárások ritkábbak, itt a Rendelet és az e-Privacy irányelv együttes alkalmazását értelmező 5/2019-es számú, vagy a tevékenységi központ, illetve letelepedési hely eljárás közbeni megváltozása esetén az illetékes hatóság megállapításáról szóló 8/2019-es számú véleményeket említhetjük.

[372] A Rendelet (148) preambulumbekezdésének utolsó mondata szerint.

révén a közigazgatási szabályok is egyfajta teszt alatt állnak, amelynek sikere vagy sikertelensége ki fog hatni a szabályozás hatékony érvényesülésére.

A Rendelet harmonizációt célzó rendelkezései két tagállamban, Dániában és Észtországban nem úgy érvényesülnek, mint a többi tagállamban, ugyanis jogrendszerük nem teszi lehetővé a Rendeletben meghatározott közigazgatási bírságok kiszabását. A közigazgatási bírságokra vonatkozó szabályok Dániában oly módon alkalmazhatók, hogy a bírságot az illetékes nemzeti bíróságok büntetőjogi szankcióként rójják ki, Észtországban pedig a felügyeleti hatóság rója ki a bírságot szabálysértési eljárás *(misdemeanour procedure)* keretében. A kiszabott bírságoknak minden esetben hatékonynak, arányosnak és visszatartó erejűnek kell lenniük.

A vitarendezési eljárás során a Testület feladata a valamely adatvédelmi felügyeleti hatóság által megfogalmazott releváns és megalapozott kifogás ügyében dönteni. A konfliktus forrása ilyen esetekben az, hogy a kifogás és a határozat tervezete eltér egymástól, és az együttműködő hatóságok nem jutottak konszenzusra a rendelkezésre álló idő alatt. A 65. cikk (1) bekezdése szerint a tagállami hatóságok közötti illetékességi vita a tevékenységi központ tekintetében szintén vitarendezési eljárás során rendezendő. A vitarendezés, valamint az illetékességi vita mellett a harmadik ügykör pedig az, amikor valamelyik felügyeleti hatóság nem kéri ki a testület véleményét a 64. cikk (1) bekezdésében meghatározott ügyekben, vagy ha ki is kéri, nem azzal összhangban jár el. Ebben az esetben bármelyik hatóság kezdeményezhet vitarendezési eljárást. A testület tagjainak kétharmados többségével kötelező erejű döntést hoz, amely köti a fő felügyeleti hatóságot és az eljárásban részt vevő valamennyi hatóságot.

Az eljárás megindításától számított két hónapon belül kétharmados többséggel születik a döntés. A határidő eredménytelen letelte után lehetőség van egyszerű többséggel döntést hozni, ahol szavazategyenlőség esetén az elnök szavazata dönt. Az eljárás részletes szabályait a 65. cikk (2)–(3) bekezdése rögzíti.

Az ilyen döntések azért is jelentősek, mert valamennyi hatóság részvételével kerül sor a döntés meghozatalára, és tulajdonképpen precedensjellegű jogforrássá válik.

A döntés kiterjed a releváns és megalapozott kifogás összes kérdésére, különösen arra, hogy a Rendelet sérült-e az adatkezelés során.

A vitarendezési eljárás funkciója végső soron az, hogy a Rendelettel összhangban álló döntés szülessen, a testületi mérlegelést igénylő konkrét kérdéseket a kifogás tartalmazza. Hasonlítható az eljárás az Európai Unió Bíróságának előzetes döntéshozatali eljárásához, ahol a döntéshozó szerv az elé tárt jogkérdésekben kötelező erejű döntésben foglal állást a tagállami eljárás egyidejű felfüggesztése mellett.[373]

A döntéshozatal alapjául szolgáló kifogásban bármilyen kérdés felvethető, így a bírsággal összefüggésben fent tárgyalt valamennyi körülmény is szóba kerülhet. A testület nem dönt egyes esetekben konkrét bírságösszegről, arról azonban állást foglalhat, hogy egy megjelölt bírságösszeg vagy összegtartomány alkalmazása megfelel-e a hatékonyság, arányosság és a visszatartó erő elvárásainak.

A testületi döntést a fő felügyeleti hatóságnak kell végrehajtania, és olyan jogerős határozatot hoznia, amely a testület döntésével összhangban van. A jogerős határozat közléséről a testületet is tájékoztatni kell.

A felügyeleti hatóságok függetlenségéről

A felügyeleti hatóságok meghatározó szerepet játszanak a védelem megteremtésében és erősítésében, erről korábban már szóltam. Mind a 95/46/EK adatvédelmi irányelv, mint a Rendelet úgy rendelkezik, hogy a hatóságok feladataikat teljes függetlenségben látják el. A teljes függetlenség kritériumait a szakirodalom és a bírói gyakorlat részletesen kimunkálta. E helyütt a teljes függetlenség követelményének rövid áttekintésére szorítkozom, majd a Rendelet által bevezetett új eljárásrend és a hatóságok függetlenségének összefüggéseit vizsgálom.

Hielke Hijmans az adatvédelmi felügyeleti hatóságok függetlenségét az Európai Központi Bank (EKB) függetlenségéhez hasonlítja. Nem állítja, hogy a függetlenség a két szerv esetében azonos lenne, mindenesetre a hasonlóság jelentős, különösen abban a tekintetben, hogy utasítást egyik szerv sem kérhet, illetve fogadhat el. Az EKB esetében ezt az Európai Unió működéséről szóló szerződés 130. cikke írja elő.[374]

[373] Az Európai Unió működéséről szóló szerződés 267. cikke szerint.
[374] Hijmans (2016): i. m. 317.

Hustinx az Európai Unió Alapjogi chartájában rögzített alapjogokat elemezve kiemeli, hogy kevés jog élvez „intézményi támogatást" *(structural support)*. Ebben a körben csupán az adatvédelem és a tisztességes eljáráshoz való jog említhető.[375] Előbbi esetében a független hatóságok létrehozatala a jog védelmének hatékonysága érdekében történt.

A függetlenség alábbi kritériumai egyrészt valamitől való tartózkodást jelentenek a kormányzatok és más szereplők oldalán. A függetlenséggel kapcsolatos követelmények azonban nem csupán tartózkodásként, hanem aktív magatartásként is meghatározhatók. A hatóságok függetlensége tehát nem kizárólag a hatóságok magatartásán múlik, hanem más szereplők, így a költségvetést meghatározó döntéshozók, a kormányzatok stb. közrehatásán is nyugszik. Másrészt mindazonáltal kulcsszerep jut értelemszerűen maguknak a hatóságoknak, amelyek felelőssége óvni saját függetlenségüket, amelynek csorbítására irányuló törekvéseket elsőként ők maguk érzékelhetik.[376] Az adatvédelmi hatóságok tehát maguk is felelősek az integritásuk megőrzéséért. Az európai adatvédelmi biztos az alapvető értékeit a pártatlanságban, pragmatizmusban, az integritásban és az átláthatóságban nevezte meg a 2015–2019-es időszakra szóló stratégiájában.[377] A jó kormányzás *(good governance)* kapcsán Ottow a törvényesség, a függetlenség, az átláthatóság, a hatékonyság és a felelősség követelményeit említi.

Nélkülözhetetlennek tartom, hogy maguk az adatvédelmi hatóságok is kiépítsék belső védelmi vonalaikat annak érdekében, hogy adott esetben konfliktusos közegben is független módon tudjanak eljárni. Ezen a téren, ahogy látjuk, az elsődleges kérdés az értékek azonosítása. Ebben a kontextusban mutatok rá a kötet mottójának tudatos megválasztására. Az ott megjelölt értékek nem csupán az Európai Unió, hanem az unió szabályainak érvényesítéséért felelős valamennyi szerv és személy számára kiinduló- és tájékozódási pontot adnak.

[375] Hustinx (2009): i. m. 133.

[376] Annetje Ottow: *Market & Competition Authorities – Good Agency Principles.* Oxford University Press, 2015. 3. fejezet.

[377] *Leading by example – The EDPS Strategy 2015–2019,* 3. Forrás: az európai adatvédelmi biztos (EDPS) honlapja.

A függetlenség kritériumai

A függetlenség kritériumait és azok tartalmát az következőkben határozhatjuk meg.

Külső befolyástól mentes feladatellátás

A hatóságok minden külső, elsősorban politikai, de bármilyen más külső befolyástól mentesen járnak el.

> Az Európai Bizottság kontra Németország ügyben (C-518/07. szám) az Európai Unió Bírósága akként foglalt állást, hogy „feladataik gyakorlása során az ellenőrző hatóságoknak objektíven és pártatlanul kell eljárniuk. Ezért minden külső befolyástól mentesnek kell lenniük, ideértve az állam vagy a tartományok által gyakorolt közvetlen vagy közvetett befolyást is, nem csak az ellenőrzött szervezetek általi befolyást" (ítélet 25. pontja).

Utasítást senkitől sem kérhetnek, illetve fogadhatnak el. A függetlenség nem csupán a felügyeleti hatósággal szembeni elvárás, hanem minden más szereplőt arra kötelez, hogy tartózkodjon a hatóságok független működésének befolyásolásától.

Az Európai Unió Bírósága szerint a „függetlenség nemcsak az ellenőrzött szervezetek által gyakorolt bármilyen befolyást zár ki, hanem bármilyen összefonódást vagy más, akár közvetlen, akár közvetett külső befolyást is, amely akadályozhatná az említett hatóságoknak a magánélet védelméhez való alapvető jog és a személyes adatok szabad áramlása közötti helyes egyensúly létrehozásában álló feladatai teljesítését".[378] A külső befolyástól való mentesség tehát a szervezeti működés egyik elsődleges alapfeltételeként jelenik meg a bírói gyakorlatban. Ennek felismerése és elhárítása a szervezet által érvényesített vezetési szempontok között előkelő helyen szerepel.

Simitis már a nyolcvanas években követelményként fogalmazta meg, hogy a felügyeleti hatóságnak minden potenciális adatfelhasználótól függetlennek kell lennie. A magán- és a közintézményektől is ugyanolyan távol-

[378] Az Európai Bizottság kontra Németország ügyben született ítélet 30. pontja szerint.

ságot kell tartania. Példaként a hesseni parlamenti biztos példáját említi.[379] Óva int vegyes összetételű bizottságok létrehozásától, ahol például a kormányzatnak és a privát szektornak is van képviselete. Az ilyen szervezetek ugyanis jó eséllyel a társadalom nyilvánossága előtt lefolytatandó vitákat belső fórum előtt, zárt körben bonyolítanák le. E szerepében a hatóság pedig azt kockáztatja, hogy bizonyos adatkezelési folyamatok és adatgyűjtési technológiák legitimálásában vesz majd részt, ahelyett hogy szükség esetén nyilvánosan bírálja a helytelen irányba mutató gyakorlatokat.[380]

Bár Spiros Simitis álláspontjával egyet tudok érteni, azt is látni kell, hogy a parlamenti biztos a törvényalkotó hatalomhoz való közelsége és más tényezők miatt olyan intézménynek bizonyult, amely nem minden tekintetben felelt meg a felügyeleti hatósággal szemben támasztott követelményeknek. Jóri 2010-ben szintén az adatvédelmi biztosi intézmény jelentős reformját és az információs biztosi intézmény létrehozását szorgalmazta.

Jóri András írásában egy ideális intézményi reform alapvonalait rajzolta meg. Az új intézmény megőrizné az ombudsman három alapvető funkcióját, így az alapjogvédelmi funkciót, az ombudsmani jogalkalmazást és mediációt, továbbá a hatósági jogalkalmazást. Ez utóbbi a titokfelügyeleti hatáskörben, továbbá az uniós jogharmonizációs célú, 2003-as novella nyomán az Avtv. szabályozásában már jelen volt. Az ideális új szabályozás egy független, közigazgatási típusú szervet képzelt el, amelynek kötelező döntéseit bíróság előtt felülvizsgálat alá lehet vonni. A javasolt új modell a többi országgyűlési biztos közös hivatalától függetlenítette volna az információs biztost, és költségvetési függetlenséget garantált volna a számára. A Jóri által javasolt szabályozás megőrizte volna a személyes adatok védelmének és a közérdekű adatok nyilvánosságának intézményi egységét, és egyaránt megőrizte volna az ombudsmani és hatósági fellépés eszköztárát. Új és fontos hatáskörként jelenik meg a bírságolás.[381]

[379] Simitis (1987): i. m. 743., 746. Írásában Simitis is elismeri, hogy a parlamenti biztos által használható eszköz, a nyilvánosság előtti vita kezdeményezése életlen eszközzé válhat, ha túl gyakran élnek vele.

[380] Vö. Jóri (2015): i. m.

[381] Jóri András: Az információvédelemért és az információszabadságért felelős biztos intézményéről. *Fundamentum,* 14. (2010), 2. 20–29.

Anyagi és szervezeti függetlenség

A teljes függetlenség kritériumai közé tartozik a Rendelet szerint az, hogy a hatóságok hatékony feladatellátásához biztosítsák a megfelelő anyagi és személyzeti forrásokat, így a helyiséget és az infrastruktúrát. A felügyeleti hatóság önálló költségvetéssel rendelkezik.

> Ez a költségvetés értelemszerűen része lehet az állami költségvetésnek, de azon belül jól láthatónak, más szervektől elkülöníthetőnek kell lennie. A Rendelet a saját, nyilvános és éves költségvetést jelöli meg a költségvetés kapcsán a hatékony működés követelményeként a (120) preambulumbekezdésben.
> A C-614/2010 számú, az Európai Bizottság kontra Ausztria ügyben az Európai Unió Bírósága a függetlenség sérülésének látta, hogy az osztrák adatvédelmi felügyeleti hatóság személyi állományába tartozó köztisztviselők fölött a kancellári hivatal szolgálati felügyeletet gyakorol (ítélet 55–66. pontjai).

A független működéssel összefér, hogy a hatóságok pénzügyi kiadásait az erre rendelt szervek ellenőrzik.[382] Soós az Európai Bizottság kontra Ausztria ügy kapcsán kiemeli, hogy a szervezeti függetlenség mércéje még a bíróságokkal szemben támasztott követelményeket is felülmúlhatja.[383]

> Jan Mazák főtanácsnoki indítványát elemezve kiemeli, hogy elképzelhető olyan eset, amikor egy nemzeti hatóság elég „független" ahhoz, hogy bíróságnak lehessen minősíteni, míg ugyanezek a kritériumok nem elégségesek ahhoz, hogy független adatvédelmi hatóságnak minősüljön. Soós konklúziója tehát az, hogy „az adatvédelmi hatóságok függetlensége az EUB gyakorlata szerint akár többletelemeket is tartalmazhat a bírói függetlenséghez képest".

Az Európai Bizottság álláspontja szerint nem csupán az egyes hatóságok számára kell biztosítani a szükséges erőforrásokat, hanem ezek egyenlőt-

[382] A Rendelet 52. cikk (6) bekezdése a pénzügyi kiadások ellenőrzéséhez hozzáteszi, hogy a „függetlenségét nem befolyásoló pénzügyi ellenőrzés" fér össze a teljes függetlenség kritériumával. A tevékenységet érdemben vizsgáló, a szakmai tevékenység érdemét érintő megállapításokhoz, valamint azok számonkéréséhez vezető ellenőrzés nincs összhangban a Rendelet betűjével és szellemével.

[383] Soós Andrea Klára: Az adatvédelmi hatóságok „teljes függetlensége": az Európai Unió Bíróságának gyakorlata. *Infokommunikáció és Jog,* (2012), 52–53. 219–223.

lensége, aránytalansága is veszélyeztetheti a hatóságok „rendeletben előírt teljes függetlenség[ét]”.[384]

A felügyeleti hatóság tagjainak függetlensége és a személyzet irányítása

A Rendelet a felügyeleti hatóság vezetőjével, illetve vezetőivel szemben szigorú feltételeket támaszt. A megválasztásra irányuló eljárásnak jogszabályban rögzítettnek és átláthatónak kell lennie. A kinevezés a kormány, a parlament vagy az államfő feladata, ez a tagállami jogalkotó döntésén múlik. A hatóság vezetője (tagja) nem végezhet olyan tevékenységet, nem tanúsíthat olyan magatartást, amely a szervezet független működését veszélyeztetné. A hatóság vezetése alá tartozik az általa kiválasztott személyzet.[385] A függetlenséggel nem fér össze, hogy a felügyeleti szerv vezetőjét feladatai ellátásával összefüggésben, jogszabályban meghatározott megbízatási idejének lejárta előtt elbocsássák.

A C-288/12 számú, az Európai Bizottság kontra Magyarország ügyben az Európai Unió Bírósága megállapította, hogy az adatvédelmi biztosi pozíció hatéves mandátumának lejárta előtti megszüntetése nem fér össze a teljes függetlenség követelményével. Amennyiben a felügyeleti szervek vezetőjét az a veszély fenyegeti, hogy idő előtt felmentik őket vagy átalakítják hivatalukat, feladataikat nem tudják külső befolyástól mentesen, függetlenül ellátni – „ilyen helyzetben nem tekinthető úgy, hogy a felügyelő hatóság a részrehajlás legcsekélyebb gyanújától mentesen működhet” (az ítélet 55. pontja szerint).

Soós arra is rámutat: nem csupán az átszervezés ténye, hanem már az átszervezés előtti időszak, az intézmény jövőjének elbizonytalanítása is közvetett és közvetlen hatással jár a hatóság által végzett munkára nézve.[386]

[384] Az Európai Bizottság közleménye az Európai Parlamentnek és a Tanácsnak: *Erősebb védelem, új lehetőségek – A Bizottság iránymutatása az általános adatvédelmi rendelet 2018. május 25-től történő közvetlen alkalmazásáról.* Brüsszel, COM(2018)43 végleges, 11. (2018. január 24.). Forrás: az EU hivatalos lapjának honlapja.

[385] A Rendelet (121) preambulumbekezdése a magyar gyakorlatban nem ismert, független szerv általi kiválasztást kifejezetten megengedhetővé teszi, míg a vonatkozó normaszöveg ezt konkrétan nem engedi meg.

[386] Soós (2012): i. m. 222.

A felügyeleti hatóságok függetlensége és kölcsönös függősége az együttműködési eljárások fényében

Fentebb utaltam már arra, hogy a hatóságok közötti együttműködés Rendeletben meghatározott eljárásai kihatnak a hatóságok függetlenségére. A hatóság függetlenségének kérdései a tagállamok szintjén szuverenitási kérdésként jelennek meg, hiszen az együttműködési és az egységességi eljárások közös hatáskörgyakorlást jelentenek. Az önállóan gyakorolt hatáskörök helyébe a közösen gyakorolt hatáskörök kerültek, ami szükségszerűen a szuverén módon hozott tagállami döntések számának csökkenésével jár.

Ez a kérdés a nemzetközi szakirodalomban is élénk vitát váltott ki.

Lynskey Európai kontextusban vizsgálja a tagállami adatvédelmi hatóságok függetlenségét *The Europeanisation of Data Protection Law* című írásában.[387] Elemzése során odáig jut, hogy a hatóságok teljes függetlensége csorbul. Kétségtelen, hogy korábban, a 95/46/EK számú adatvédelmi irányelv ideje alatt is volt lehetősége például az Európai Bizottságnak kötelezettségszegési eljárást indítani az ellen a tagállam ellen, amely nem megfelelően alkalmazta az Európai Unió jogát, azonban ez a lehetőség a tagállami hatóságok egyedi döntéseivel csak áttételesen hozható összefüggésbe. Ennek megfelelően, a korábbi szabályozásra visszatekintve nem lehet a Bizottság e hatáskörét a teljes függetlenség korlátjának tekinteni.

Lynskey álláspontom szerint helyesen mondja ki, hogy a függetlenség és a szuverenitás jelentős intézményi átrendeződéséről van szó. Ezt az átrendeződést a Rendeletet megelőző jogalkotási folyamat során az Európai Adatvédelmi Testület elődje, a 29. cikk szerinti munkacsoport is észlelte, és már 2012-ben, a WP 191-es számú véleményében[388] hangot adott aggodalmának, amely szerint az együttműködési és az egységességi eljárások nem járhatnak a nemzeti adatvédelmi hatóságok függetlenségének sérelmével.

A korábban tárgyalt eljárások elemzése révén arra jutottam az „Együttműködési eljárások és vitarendezés, hatóságok függetlensége" című fejezetben, hogy ez a függetlenség mégis korlátozás alá esik.

[387] Orla Lynskey: The 'Europeanisation' of Data Protection Law. *Cambridge Yearbook of European Legal Studies,* 19. (2017). 252–286.

[388] 2012/1. sz. vélemény az adatvédelmi reformjavaslatokról, elfogadás időpontja: 2012. március 23. WP 191. Forrás: az Európai Bizottság honlapja.

Egyet tudunk érteni Hijmans következtetésével is. E szerint a tagállami adatvédelmi hatóságok nem szuverén módon járnak el az adatvédelmi ellenőrzéseik és hatásköreik gyakorlása során, amennyiben együttműködési és egységességi mechanizmuson keresztül születnek a döntések.[389]

Wojciech Wiewiórowski[390] szintén amellett érvel, hogy a hatóságok közötti együttműködés során mindenkinek figyelembe kell vennie a közös célokat, nem csupán a saját szempontjainak érvényesítésére kell törekednie. Akár európai, akár globális téren működnek együtt a hatóságok, a közös érdekeket kell keresni, csak így lehet erősíteni az adatalanyok helyzetét.[391]

Wojciech Wiewiórowski 2015–2019 között az európai adatvédelmi biztos helyettese, 2010–2014 között pedig Lengyelország adatvédelmi hatóságának, a GIODO-nak volt az elnöke. 2019 novemberében az Európai Bizottság javaslatára az Európai Unió Tanácsa és az Európai Parlament közös döntésével öt évre európai adatvédelmi biztossá választotta.

Konklúzió – hatóságok függetlensége a védelmi lépcső fényében

A függetlenséget illető következtetésem egybecseng Lynskey következtetésével, aki rámutat arra, hogy adott esetben egy vitarendezési eljárás során a tagállami hatóság arra kényszerül, hogy a testület döntése nyomán olyan határozatot hozzon, amelynek tartalmával nem ért egyet. Itt tehát már nem egyéni, hanem közös hatáskörgyakorlásról van szó. A függetlenség hangsúlyozása a tagállami szinten viszonylagos akkor, amikor az együttműködési és az egységességi mechanizmus keretében közös döntések születnek.

A függetlenség lényeges garancia marad, de ez az együttműködési eljárásokban kollektív módon érvényesül: az együttműködési eljárásokban

[389] Hijmans (2016): i. m. 371. "This sharing of powers may result in a situation where a DPA is no longer sovereign in taking decisions within its jurisdiction in individual cases, because the cooperation as laid down by law requires decisions to be taken by another DPA or […] by an institutional cooperation mechanism."

[390] Foreword – European and International Cooperation in Enforcing Privacy – Expectations and Solutions for a Reinforced Cooperation. In Paul de Hert – Dariusz Kloza – Paweł Makowski (szerk.): *Enforcing Privacy: Lessons from Current Implementations and Perspectives for the Future*. Warsaw, Wydawnictwo Sejmowe, 2015. 12.

[391] Vö. De Hert – Kloza – Makowski (2015): i. m. 12.

a vezető és az érintett hatóságok közössége jár el függetlenül; az egységességi mechanizmus során pedig a testület. A teljes függetlenség igénye és garanciája tehát a hatósági működés szükségszerű velejárója marad. A tagállami szinten érvényesülő függetlenség mellett a közös hatáskörgyakorlás szükségszerűen követel helyet a függetlenség új dimenziójának: a tagállami hatóságok közösségének szintjén is.

A kollektív függetlenség azonban elképzelhetetlen, ha az egyes tagállami hatóságok nem tudják megőrizni függetlenségüket. A hatóságok léte, amint bemutattam, a védelem rendszerében fontos és pótolhatatlan építőelemet jelent. Kérdés, hogy az adatvédelmi felügyeleti hatóság be tudja-e tölteni ezt a szerepét, ha függetlenségét nem tudja megőrizni. Álláspontom szerint a függetlenség elvesztése annak a képességnek az elvesztésével is jár, hogy egyes ügyeket a hatóság tárgyilagosan meg tudjon ítélni, és hatásköreit pártatlanul gyakorolja. Ez pedig arra vezet, hogy alapvető képességeitől fosztják meg a hatóságot. A fenti elemzés fényében a függetlenség elveszítése a védelmi lépcsőn egy óriási visszalépést, zuhanást jelent, ugyanis a hatóságra, abban a szerepében, ahogyan az uniós és nemzetközi dokumentumokból kiolvasható, nem lehet számítani. A függetlenségében sérült hatóság révén a védelem teljes rendszere sérül. Az ilyen módon kompromittálódó védelem nem tekinthető valós védelemnek.

Az Európai Bizottság rámutat arra, hogy nem csupán az egyes hatóságok helyzete, hanem az egymáshoz képest megállapítható egyenlőtlenségek is károsan hathatnak a feladatellátás és a hatáskörgyakorlás hatékonyságára. A Bizottság „a pénzügyi erőforrások közötti viszonylagos aránytalanság" elemzése során állapítja meg, hogy ez a hatékonyság rovására megy-e, „végső soron pedig a rendeletben előírt teljes függetlenségüket" is gátolhatja.[392]

Mind a pénzügyi, mint a közös hatáskörgyakorlás kapcsán arra a következtetésre jutunk tehát, hogy a tagállami adatvédelmi felügyeleti hatóságok egymástól már nem függetlenek, hanem kölcsönös függőségben állnak és működnek egymással. A hatóságok feladat- és hatáskörének elemzése során utaltam arra, hogy az egyes hatóságok is törekednek a Rendelet egy-

[392] Az Európai Bizottság közleménye az Európai Parlamentnek és a Tanácsnak: *Erősebb védelem, új lehetőségek – A Bizottság iránymutatása az általános adatvédelmi rendelet 2018. május 25-től történő közvetlen alkalmazásáról.* Brüsszel, COM(2018)43 végleges, 11. (2018. január 24.). Forrás: az EU hivatalos lapjának honlapja.

séges alkalmazására.[393] Már ez a jogalkotói elvárás is magában foglalja, hogy a Rendeletet egymással együttműködve, kompromisszumos megoldásokra törekedve kell alkalmazni. Másként ez a jogalkotói elvárás nem lenne értelmezhető.

Arra jutunk tehát, hogy az egységes értelmezés áldozatot kíván a hatóságok egymástól való függetlensége terén, mert ez az egyetlen lehetőség arra, hogy a Rendelet egységes értelmezése és harmonizált alkalmazása megvalósulhasson. Rá kell mutatni arra, hogy a jogalkotó itt egy döntés előtt állt: vagy elfogadja a Rendelet előtti modellt, amelyben az egyes tagállami hatóságok egymástól is függetlenül értelmezték és alkalmazták a közös szabályokat, vagy csorbítja a hatóságok egymással szembeni függetlenségét, és megteremti a közös hatáskörgyakorlás és a kölcsönös függőség modelljét. Az Európai Parlament és a Tanács az utóbbi modellt választotta, amelynek célja az, hogy a Rendelet egységes módon biztosítsa az érintetti jogokat, és a közös piac elvárásának megfelelően minden tagállamban azonos versenyfeltételeket teremtsen minden szereplő számára. A tisztességes verseny feltételeinek megteremtése túlmutat a szűk értelemben vett adatvédelmen, de nem választható el attól.

Az EDPS 2014-ben kiadott előzetes véleménye az *Adatvédelem és versenyképesség a big data korában: Az adatvédelem, a versenyjog és a fogyasztóvédelem kölcsönhatása a digitális gazdaságban (Privacy and Competitiveness in the Age of Big Data: The Interplay Between Data Protection, Competition Law and Consumer Protection in the Digital Economy)* címmel szorgalmazza a privacy szempontjainak versenyelőnyként való megjelenítését, ugyanakkor megállapítja, hogy „a digitális gazdaságban működő cégek a privacy védelmét egyelőre nem tekintik versenyelőnynek" (33.). Felhívja egyszersmind a figyelmet a személyes adatok értékére a digitális gazdaságban, amely jelentős potenciállal rendelkezik az értékteremtésben, és fizetőeszközként is funkcionál. E ténynek jelentős következményei vannak olyan kulcsfogalmak értelmezése terén, mint az átláthatóság, a piaci dominancia, a fogyasztói jólét és a kár (37.).[394]

[393] A Rendelet 51. cikk (2) bekezdése szerint „minden felügyeleti hatóság elősegíti e rendeletnek az Unió egész területén történő egységes alkalmazását. A felügyeleti hatóságok e célból együttműködnek egymással és a Bizottsággal, a VII. fejezettel összhangban."
[394] Az európai adatvédelmi biztos (EDPS) honlapja. *Edps.europa.eu.*

A közös hatáskörgyakorlás intézményi reformja – az előrelépés lehetősége

A függetlenség problematikája körében meg kell említenünk egy olyan lehetséges szervezeti megoldást, amely kiküszöbölhet bizonyos függetlenségi deficiteket. Ez pedig az együttműködési eljárások újabb szintre emelése egy közös európai uniós adatvédelmi hatóság révén. E ponton meg kell említeni, hogy a tagállami hatóságok rendkívüli figyelmet szenteltek és érzékenységet mutatnak akkor, amikor a független működés feltételeit szabályozzák. Az Európai Bizottság által 2012 januárjában benyújtott javaslat kapcsán bizalmatlanság érződött a szabályozás tervezetével kapcsolatban, amikor az európai adatvédelmi biztosnak állandó alelnöki pozíciót írtak volna elő. A testület titkárságát szintén az európai adatvédelmi biztos adja, és ennek részleteit már korán tisztázni szerette volna az adatvédelmi hatóságok közössége, különös tekintettel arra, hogy a titkárságot a testület egyik tagja nyújtja.[395] A jelenlegi szabályok szerint az egyablakos ügyintézés körébe eső esetekben a releváns és megalapozott kifogást követően a vitarendezés a testület hatáskörébe tartozik. Ezt tekinthetjük kollektív hatáskörgyakorlásnak, azonban több szempontból is esetleges, hiszen több feltétel együttes fennállása esetén kerül csak sor rá: ha az eljáró hatóságok közötti vita valóban nem zárul kompromisszumos megoldással, és még ebben az esetben is csak azok a kérdések kerülnek a testület elé, amelyek a releváns és megalapozott kifogásban szerepelnek.

Egy elképzelt európai uniós adatvédelmi hatóság eljárhatna minden olyan jelentősebb ügyben, amelyben határon átnyúló adatkezelésekről van szó. A döntéshozatalt a testület mellett működő jogi szolgálat készíthetné elő, természetesen mindazon tagállami hatóságok számára követhető és transzparens módon, amely véleményét már ebben a fázisban is hangoztatni szeretné. A döntéshozatal pedig a testület előtt, a vitarendezésre egyébként irányadó szabályok szerint folyhatna. Miben jelentene előrelépést ez a megoldás?

Az ilyen döntéshozatal kedvezően hatna a hatóságok közötti együttműködésre, hiszen nagyszámú ügyben kellene közös döntéseket hozniuk. Önmagában az együttműködés megvalósulása előrelépést jelent a védelem

[395] A 29. cikk szerinti munkacsoport 2012/1. sz. véleménye az adatvédelmi reformjavaslatokról, WP 191, elfogadás időpontja: 2012. március 23. 22. Forrás: az Európai Bizottság (a 29. cikk szerinti munkacsoport titkárságának) honlapja.

szövetének erősítésében. Szintén előrelépést jelentene a Rendelet egységes alkalmazásában, hiszen nagyobb számú ügyben kerülne sor kollektív döntéshozatalra. A transzparens döntéshozatalt szintén erősítő mechanizmus lenne ez a szoros együttműködés, amely a hatóságok működésében is kedvező gyakorlatokat generálhatna. Az érintetti joggyakorlás terén a közös eljárások nem feltétlenül lennének lassabbak, mint a jelenlegi jogi keretben, bár ennek kockázatával számolni kell. Ami viszont a jogorvoslatot illeti, ott bizonyosan javulna az érintett helyzete, hiszen csak egyetlen eljárásrend keretében, nevezetesen az uniós döntéshozatal keretében[396] szembesülne az adatkezeléssel összefüggő döntés megtámadhatóságának problémájával. Ez a megoldás még mindig nem a hazai fórum lenne, de a jelenlegi széttöredezett struktúra[397] helyett egy csatornát kínálna az Európai Unión belül. Végül pedig a döntések hitelessége is erősödhet, hiszen a közös, a működés helyétől független fórum előtti döntéshozatal felül állna minden olyan találgatáson, amely a tevékenységi központ és a helyi kormányzatok, hatóságok közötti, kívánatosnál is erősebb kölcsönös szolidaritás kapcsán esetlegesen megfogalmazódhat.

[396] Ebben az esetben a közös hatóságot mint uniós szerv döntését vizsgálnák felül az Európai Unió Bírósága előtt.

[397] A Rendeletben meghatározott eljárásrend szerint az érintett minden esetben csak a döntéshozatal helye szerint kereshetne jogorvoslatot az általa sérelmesnek tartott hatósági határozattal szemben.

Vákát

Végkövetkeztetések

Amint azt a bevezetésben említettem, a kutatás során arra a kérdésre kerestem a választ, hogy a személyes adatok védelmének szintje jogi eszközökkel meghatározható-e, illetve a védelem egyes szintjei definiálhatók-e. Amennyiben igen, úgy melyek azok a kritériumok, amelyek alapján az egyes szintek között minőségi különbség tehető? Mi az egyes szintek közötti összehasonlítás alapja? Mindezek fényében milyen lehetőségek adódnak a védelem szintjének alakítására, milyen jogi eszközökkel javítható a védelem minősége?

A védett jog tartalma

Az elemzésben számos döntésen keresztül vizsgáltam az Európai Emberi Jogi Bíróság esetjogát. Témánk szempontjából ez azért releváns, mert az EU Alapjogi chartája szerint a chartában biztosított jogok tartalmát és terjedelmét azonosnak kell tekinteni azokéval, amelyek az Egyezményben szerepelnek. Ilyen értelemben a strasbourgi esetjog minimum védelemként értelmezhető.

A védelmi lépcső elmélete

Az elemzés középpontjában a felvetett kérdésekre válaszolva egy olyan szempontrendszer, a védelmi lépcső elméletének megalapozása áll, amely a védelem szintjének elemzése során jogi értelemben is megragadható szempontokat nyújt.

A védelmi lépcsőn nem szükséges sok fokozat azonosítása. A lépcső elméletében egy felfelé a végtelenbe mutató, lineáris lépcsőt képzelünk el, amely a védelem javulásának és alkalmazkodásának kifogyhatatlan lehetőségét jeleníti meg a jövőben. Egzakt módon sem a lefelé, sem a felfelé vezető fokok nem határozhatók meg nagy számban, három szint meghatározása azonban elengedhetetlen. Az első az a fokozat, amelyen a védelem szintje jelenleg megragadható. A második az, amelyikről a jelenlegi szintre felfelé, vagy éppen lefelé lépett a védelem. A harmadik szint pedig a kívánatos, előrelépésnek tekinthető védelem szintje. Szükséges, hogy a két fok között a különbséget egyértelműen meg tudjuk határozni.

A védelem komponensei és minőségi mutatói

Fentebb részletesen áttekintettem azokat a komponenseket, amelyekből a védelem rendszere áll. Ezt követően azonosítottam azokat a minőségi különbségeket, amelyek az egyes fokok között húzódnak. Miben áll a minőségi különbség két fokozat között?

E tekintetben – elemzésem szerint – amint azt „A védelmi lépcső fokozatainak azonosítása" című fejezetben bemutattam – számos tényező jöhet szóba. A minőségi javulás indikátora lehet, ha az érintett jogai bővülnek, vagy a jogok változatlan katalógusa mellett is javul a jogérvényesítés lehetősége. Amikor az érintett számára elérhető információk köre bővül, vagy a szabályozás e tekintetben világosabb követelményeket határoz meg, szintén minőségi javulás történik.

Az előrelépés jellemzője, hogy az adatkezelőket az adatkezelés kapcsán terhelő kötelezettségek az alkalmazott technológia és az üzleti modellek fejlődésével párhuzamosan változnak.

Az adatvédelmi hatóságok mozgástere, feladat- és hatásköre szintén minőségi jellemzője a védelem szintjének. A hatóságok feladatainak, hatásköreinek bővülését önmagában is minőségi változásnak tekinthetjük megjegyezve, hogy a hatóságok hatékony működése jeleníti meg a kedvező eredményt a védelmi lépcső tükrében. A minőségi előrelépés megmutatkozhat a jog hatékonyságában is. Az adatvédelmi jog hatékonyságának jogi fokmérője, hogy a magánszféra védelme erősödik, fejlődik.

A minőségi fejlődés fontos fokmérője, hogy az adott változás képes-e hozzájárulni az adatvédelmi kultúra kialakulásához, illetve fejlődéséhez.

Amennyiben ez megvalósul, úgy a védelmi lépcsőn előrelépés történik.

Az adatvédelmi tisztviselő szerepének megújításáról a védelmi lépcső fényében

Az adatvédelmi tisztviselő, szerepéből adódóan – Le Métayer szemléletes elemzését alapul véve – az egyén, a jogi, az informatikai szakma és a piaci szereplők mindegyikéhez közel áll. Tevékenysége során a magánszférát érintő kockázatokat figyelembe veszi, és e kockázatok alapján határozza meg munkájának prioritásait.

Az adatvédelmi tisztviselői intézmény meghonosítása jelentős előrelépés a védelem terén. A statikus védelmi komponensek között határoztam meg azt, amelynek esetében leginkább a létrehozatal előtti és az azt követő szintet különböztetjük meg. Ez nem zárja ki annak lehetőségét, hogy a már létező szabályozást és működést továbbfejlesszük, és a védelmi lépcső fényében meghatározzuk az előrelépés lehetőségeit. „Az adatvédelmi tisztviselő feladatai és jogállása a védelmi lépcső elméletének fényében" című fejezetben konkrét javaslatokat fogalmaztam meg ezen a téren is.

Álláspontom szerint az adatvédelmi tisztviselői pozíciót tovább kell erősíteni, professzionalizálni szükséges, és egy sokkal kötöttebb rendben kell elfoglalnia a helyét az adatkezelő szervezeten belül. A jogalkotás terén előremutató lépésekre van szükség, hogy ez megvalósulhasson.

Végrehajtási rendeleti szabályozási lehetőséget akár az Európai Adatvédelmi Testülethez is lehetne telepíteni.

A szabályozás rész lehetne egy vizsga, amely uniós szinten egységes elvárások szerint zajlik, kiegészülve a szakmai egyesületi tagsággal.

Az Európai Unió intézményeiben foglalkoztatott adatvédelmi tisztviselők munkajogi védelme példamutató hiszen a tisztviselő csak akkor bocsátható el állásából idő előtt, ha azt a hatóság is jóváhagyja. Ez a függetlenséget szolgáló pótlólagos védelem kiegészíthető a határozott idejű kinevezéssel, amely jobban megfelel a munkaerőpiac követelményeinek.

Javasolt, hogy amennyiben a tisztviselőt foglalkoztató adatkezelő szervezet új adatkezelést kíván bevezetni, és ezt a tisztviselő ellenzi, úgy azt be kell jelenteni az adatvédelmi hatóságnak. Olyan mélységű ellenőrzést jelentene ez, amelyre az adatvédelmi hatóságok a jelenlegi modell szerint képtelenek lennének.

Szükséges az új tisztviselői szerep kialakítása a leírt védelmi deficit ellensúlyozására. Erősíteni kell a transzparenciát, a konfliktusbejelentési kötelezettség nem jelentene aránytalan adminisztratív terhet. Olyan többletet jelentene mégis a felügyelet során, amely más forrásból nem pótolható.

Kétségtelen, hogy jelentős változással járna ez a tisztviselő és az adatkezelő együttműködésében, de a lehetséges konfliktusok ellenére is az egyik lehetséges és működőképes új modellnek tartom.

Az adatvédelmi felügyeleti hatóság feladatellátásának új modellje a védelmi lépcső alkalmazásával

A Rendelet a hatóságok számára egyenrangú feladatokat határoz meg, ezek között viszont kiemelt szerep jut az érintetti panaszok kezelésének. A Rendelet nevesíti is azt, hogy az érintett jogosult a felügyeleti hatósághoz panasszal fordulni. A felügyeleti hatóságok által e körben ellátott feladatok mennyisége tehát nagymértékben függ a beérkező panaszok számától.

Egyik oldalon a panasztételhez való jog az érintett erős jogosultsága, másik oldalon pedig annak jele, hogy a Rendelet nem megfelelően érvényesül. E két jelenség kéz a kézben járnak egymással. Arra a következtetésre jutottam, hogy a jogalkotói cél a minél kevesebb jogsértés, ebből következően pedig a panaszok száma ideális esetben alacsony. Felmerül a kérdés: milyen módon lehetne elérni azt az állapotot, hogy a panaszok száma csökkenjen, és ez együtt járjon az adatvédelmi jog hatékonyságának javulásával?

A hatékony feladatellátás kapcsán javasoltam a panaszokat megelőző stratégiát. Ha a hatóság nem a panaszokat követő, hanem a panaszokat megelőző stratégiát követ, sokkal nagyobb hangsúly jut az utóbbi feladatoknak.

A koncentrált adatkezeléssel és sok konfliktushelyzetet magában hordozó jogviszonyokra összpontosítva a hatóságoknak javasolt lenne olyan programokat indítani, amelyek célja az adatkezelő kezébe megfelelést könnyítő eszközöket adni. Az adatkezelők, illetve adatkezelők szövetségei, érdekképviseleti szervei ilyen módon a hatósággal partnerségben alakíthatnák adatkezeléseiket, szabályzataikat, belső eljárásrendjüket. A magánszférát érintő megfontolásokon túlmutató érvek is felhozhatók e modell mellett, hiszen társadalmi szinten sokkal gazdaságosabb egy ilyen rendszer fenntartása. A jelenleginél hatékonyabb modell lenne ez, amely a védelmi lépcsőn is mérhető előnyökkel járna.

Az adatalanyok oldalán ez azzal az előnnyel jár, hogy az adatkezelők nagyobb eséllyel fognak nemcsak jogkövető módon, hanem jogi kérdésekben tájékozottan eljárni. Az adatkezelő oldalán a jogbiztonság erősödik, és a modell sikere révén egy idő után csökkenne a panaszok száma, hiszen a konfliktusos helyzeteket el lehetne kerülni, vagy egyszerűbben meg lehetne oldani.

Az új modell kedvező hatása a költségek csökkenésében is mérhető, továbbá a magánszféra körében megvalósuló jogsértések számának csökkenésében is megragadható. A jog hatékonyságának körében tett fenti kitérő alapján ez az érdemi értéke és többlete az új modellnek.

A felügyeleti hatóságok hatáskörének elemzése a védelmi lépcső alapján

A felügyeleti hatóságok hatáskörének rendeleti szintű rögzítése jelentős mértékű egységesítést hozott magával. A tagállami jogalkotó helyett az uniós jogalkotó határozta meg a pontos és tételes hatásköri katalógust.

A védelmi lépcsőt alapul véve arra jutottam, hogy önmagában az, hogy az adatvédelmi hatóságok hatásköre szélesedik, olyan mozgástértöbbletet hoz, amelyet a védelem szempontjából minőségi előrelépésként értékelhetünk. Az irányelvi szabályozással összevetve a minőségi előrelépés abban ragadható meg, hogy a Rendelet az új hatáskörök révén gyakorlatilag minden olyan életviszonyba beavatkozási lehetőséget biztosít a hatóságok számára, amely a magánszféra védelmét érintheti.

A védelmilépcső-elmélet fényében minőségi javulásként tartandó számon, hogy a hatóságok bővülő hatásköre révén javul a jogérvényesítés lehetősége. Szintén minőségi előrelépést jelent a hatáskörök tekintetében az, hogy a hatósági mozgástér bővülése világosabb szabályozási környezetet eredményez, ennek révén az adatkezelők oldalán is egyértelmű, hogy milyen esetekben avatkozhat be a hatóság. A Rendelet új hatásköri szabályai a védelmi lépcsőn minőségi előrelépésként értékelendők, az irányelvvel való összehasonlítás, valamint a védelmi lépcső által elvárt minőségi jellemzőkkel való összevetés is ezt mutatja. A védelmi lépcső két fokát ilyen módon meg tudtuk határozni, az első a Rendeletet megelőző időszakot jellemezte, míg a második szintet maga a Rendelet jeleníti meg.

Milyen módon lehetne a védelmi lépcső következő szintjét meghatározni? Álláspontom szerint a hatáskörök rendszeres felülvizsgálata és karbantartása szükségszerűen fogja a jelenlegi védelmi szintet legalábbis fenntartani, vagy újabb szintváltást nem eredményező módon megőrizni.

A meglévő különbségek a tagállami közigazgatási eljárási szabályok között több kérdést is felvetnek. A Rendelet hiányossága, hogy az anyagi jogi szabályok mellett nagyon kevés a harmonizált eljárásjogi követelmény. A Rendelet hatékony érvényesítését rábízza a tagállami jogalkotóra akkor, amikor minimális eljárási szabályokat sem épít be a kikényszerítés szabályrendszerébe.

A védelmi lépcsőn az jelent előrelépést, ha majd a hatáskörgyakorlás is a tagállamok által meghatározott közös szabályrendszer szerint valósul meg. A Rendeletet közigazgatási kódexszel, vagy legalább minimális eljárási garanciarendszerrel kell kiegészíteni. Enélkül nem számíthatunk arra, hogy a harmonizált hatásköri lista harmonizált gyakorlathoz vezet

a tagállamokban. Enélkül pedig egy olyan hatékonysági deficittel kell számolnunk, amely a védelmi lépcső elért fokát rendkívül törékennyé teszi, folyamatos visszacsúszás fenyegeti. Azzal is számolni kell, hogy az uniós jogalkotás a tagállami jogalkotásnál lényegesen lomhább, ezért a védelmi lépcsőn érvényesülő, felfelé mutató „gravitáció" sem képes ezt a hiányosságot olyan időn belül ellensúlyozni, hogy az ne járhatna valós védelmi veszteséggel.

Ennek kapcsán fogalmaztam meg azt a javaslatot, hogy az egyablakos ügyintézésnél szorosabb, közös mechanizmusban döntsenek a hatóságok a határon átnyúló ügyekben. Egy elképzelt európai uniós adatvédelmi hatóság eljárhatna minden olyan ügyben, amelyben határon átnyúló adatkezelésekről van szó. Ezen a ponton nyitva kell hagyni azt a kérdést, hogy milyen súlyú ügyeket célszerű ebbe a típusú eljárásba bevonni. A döntéshozatalt a testület mellett működő jogi szolgálat készíthetné elő, természetesen mindazon tagállami hatóságok számára követhető és transzparens módon, amelyek véleményüket már ebben a fázisban is hangoztatni szeretnék. A döntéshozatal pedig a testület előtt, a vitarendezésre egyébként irányadó szabályok szerint folyhatna. Ez a javaslat az eljárási szabályok hiányosságait is pótolhatná bizonyos mértékben.

Az adatvédelmi bírság elemzése a védelmi lépcső elmélete alapján

Amint fentebb részletesen elemeztem, az uniós jogalkotó az egyes tagállamokban biztosított védelmi szintet eltérőnek látta, és ezt arra vezette vissza, hogy a Rendelet által hatályon kívül helyezett 95/46/EK adatvédelmi irányelv tagállami átültetése és gyakorlata országonként eltérő volt. Annak érdekében, hogy a személyek magas szintű védelme szavatolható legyen, többek között a bírságolás terén is egységesítette a szabályozást és a tagállami hatóságok hatáskörét. A Rendelet ezen újítását a védelmi lépcső fényében előrelépésként értékelhetjük, mert a kötelezettségek az alkalmazott technológia és az üzleti modellek fejlődésével párhuzamosan változnak. A hatóságok a bírság révén értékelni tudják az új üzleti megoldásokat, azok hatását a magánszférára. A pénzügyi szankció a védelmi lépcső több minőségi indikátora tekintetében is kedvező eredményt mutat. A jogérvényesítés esélye javul, a pénzügyi kockázat egyértelmű ösztönző a jognak való megfelelés terén. A Rendelet által is bevezetett magas összegű bírság tekinthető hatékonyságot növelő ösztönzőnek.

A védelmi lépcső alapján *de lege ferenda* javaslatokat is megfogalmaztam, így előrelépést jelentene álláspontom szerint, ha nem csupán egy elméleti plafonig, hanem a kár mértékéig terjedhetne a kiszabható bírság. Nem fogadható el ugyanis, hogy az adatok jogellenes kezelése révén az adatkezelő gazdagodhasson. Ennek lehetőségét a jelenlegi szabályozás nem zárja ki. Emellett pedig a kár enyhítése terén tett intézkedéseket is megfelelő súllyal kell figyelembe venni.

Szintén javasoltam, hogy ne csupán a ténylegesen érintett személyeket vegyék számba a bírság megállapítása során, hanem mindazokat, akikre a jogellenes cselekmény irányult. Ehhez részben kapcsolódik az a javaslat, hogy a hatósággal szembeni transzparencia szabályait fordítsuk meg. Ne az számítson enyhítő körülménynek, ha a bejelentő a hatóságot egy jogsértőnek tűnő gyakorlatról tájékoztatja, hanem az számítson súlyosító körülménynek, ha ezt elmulasztja megtenni. Ebben az adatvédelmi tisztviselőnek is van szerepe.

A védelmi lépcső fényében javasoltam, hogy a bírsággal sújtható személyi kört bővítse a jogalkotó, így az adatvédelmi tisztviselő új szerepében a transzparenciához kötődő kötelezettségeinek elmulasztása esetén bírsággal is büntethető legyen. A közhatalmi szervek bírságolása terén pedig arra tettem javaslatot, hogy a szerv vezetője is szankcionálható legyen olyan esetekben, amikor a szervezetet ért kárért való helytállása elvárható. A cél ebben az esetben is a személyes felelősség erősítése, annak ellensúlyozásaként, hogy a felelősség sok esetben elmosódik a jogsértések kapcsán.

A bírságolás terén a *forum shopping* jelenségének elkerülése érdekében az is nélkülözhetetlen, hogy a tagállami hatóságok hasonló ügyekben hasonló bírságokat állapítsanak meg. E feltétel nélkül nem valósul meg a védelmi szintek egyenlősége a tagállamok között, és a védelem eróziója megindul, ami szükségszerűen a Rendelet által megalkotott rendszer széttöredezéséhez vezet.

Az adatvédelmi bírság terén is kirajzolódik tehát az azonosítani javasolt három szint, nevezetesen az irányelvi szabályozást jellemző széttöredezettség és alacsonyabb szintű védelem, a Rendelet által megállapított védelem, amely egységes és szigorú szabályai révén magasabb védelmet kínál, végül pedig a javasolt módosítások figyelembevételével a következő, magasabb védelmi szint. Következtetésem az, hogy hiába áll kézzelfogható közelségben hozzánk a magasabb védelmi szint, amikor a *forum shopping* révén a széttöredezettség és az alacsonyabb védelmi szint felé a visszacsúszás lehetősége is elképzelhető.

Az adatvédelmi hatóságok szerepéről

Az adatvédelmi felügyeleti hatóságokra gyakran úgy tekintenek, mint a személyes adatok védelméhez fűződő jog legfontosabb védelmezőire. De Hert és szerzőtársai azon az álláspontón vannak, hogy „a mindennapokban a magánszféra körében érvényesülő adatvédelem" terén a „hatékony védelem legnagyobb terhe" a hatóságok vállán van.[398] Ezzel az állítással nem tudok egyetérteni. Még ha el is fogadjuk, hogy a személyes adatok védelme terén a felügyeleti hatóságok fontos szerepet játszanak, ahogyan arról fentebb részletesen értekeztem, nem szabad túlbecsülni a hatóságok mindennapi adatkezelői döntésekben játszott szerepét, egyszerűen annál a ténynél fogva, hogy azokat nem a hatóságok hozzák meg. Itt is megmutatkozik a Rendelet fontos újításának, az elszámoltathatóság elvének szerepe, amely arra kötelezi az adatkezelőt, hogy a jogszabályoknak való megfelelés mellett is legyen képes a megfelelés bemutatására.

A Rendelet szabályozási koncepciója egyértelműen abba az irányba mutat, hogy kiemeli az adatkezelői felelősséget. Ezt csupán erősíti, támogatja a hatósági hatáskörök bővítése és egységesítése. Mindazonáltal a hatékony hatósági működés fontos ösztönző a jogszabályoknak való megfelelés terén. Az adatvédelmi kultúra fejlesztésében is sokat tehet a hatóság, amely aztán a napi döntések és gyakorlatok terén is megmutatkozik. Mindezek azonban nem járnak azzal, hogy a védelem „legnagyobb terhét" a hatóságok viselnék. Amint bemutattam ugyanis, más a funkciójuk. Valamennyi szereplőnek, így különösen az adatkezelőknek is kötelessége a Rendelet alkalmazása és hatékony érvényesítése, amelynek eredménye a védelmi szint erősödése. Ez a jogalkotói cél csak akkor érvényesül, ha az adatvédelmi intézményrendszer hatékonyan működik.

Fentebb elemeztem, hogy mindebben milyen része van az adatvédelmi felügyeleti hatóságoknak. Hasznos lesz az elemzést több adat, nagyobb gyakorlati tapasztalat birtokában is elvégezni a következő években. Amennyiben az adatvédelmi felügyeleti hatóságok számára például az adatvédelmi tisztviselői intézmény leírt továbbfejlesztése révén nagyobb mozgástér adódik a beavatkozásra, úgy a hatósági szerep értelemszerűen jelentősen átalakulhat, és a hatóság még meg nem valósult jogsértések megelőzésében

[398] De Hert – Kloza – Makowski (2015): i. m. 23.

is gyakorolhatná hatáskörét. Ennek hiányában egyelőre az előzetes beavatkozás lehetősége nagyon csekély, ez pedig megerősíti azt az állítást, hogy a napi döntések „terheiben" a legnagyobb arányt továbbra is az adatkezelők fogják viselni.

A látencia tagadása – nagyobb adatkezelői transzparencia

Előremutató gyakorlat lenne, ha az adatkezelések terén egy új modell valósulhatna meg. Az új modell középpontjában az önként vállalt transzparencia, a *látencia tagadása* állna, amelynek lényegét abban ragadhatjuk meg, hogy a kötelezően elvárt szintnél jóval magasabb mércét állítana magának az adatkezelő, és már az adatkezelést megelőző döntését is átláthatóvá tenné, lehetővé téve minden érdeklődőnek és érintettnek, hogy ahhoz hozzászólhasson.

Ez a követelmény egybecseng Ann Cavoukian *privacy by design* elveivel is. Cavoukian amellett szállt síkra, hogy az adatkezelési műveleteknek a felhasználók számára is átláthatóknak kell lenniük.[399] Amennyiben a személyes adatok védelme terén előrelépést szeretnénk elérni, úgy a transzparencia tekintetében mindenképpen javítani kell a jelenlegi gyakorlatot.

> Ez az elvárás már a korábbi évtizedekben is megjelent, örökzöldnek tekinthető. A SWIFT adatkezelése kapcsán szintén megfogalmazódott az az elvárás, hogy ahogyan a pénz útját követhetővé és láthatóvá kell tenni, úgy az adatok útját sem veheti körül homály.[400]

Az új technológiák, így a mesterséges intelligencia alkalmazása különös körültekintést vár el az adatkezelőktől, ennek részeként felelős döntéseket kell hozniuk, amelynek egyik aspektusa a transzparencia.

[399] Ann Cavoukian: *Privacy by Design in Law, Policy and Practice – A White Paper for Regulators, Decision-makers and Policy-makers*. Ontario, Information and Privacy Commissioner, 2011. 8.

[400] Vö. Szabó Endre Győző: A SWIFT adatkezeléséről. *Jogi Fórum,* 2006.

A Centre for Information Policy Leadership (CIPL) az elszámoltathatóságot és a felelős adatgazdálkodást/adatkezelést (data stewardship) hangsúlyozza. A mesterséges intelligencia körében az elvek, értékek, folyamatok definiálása kulcskérdés. Elvi jelentőségű a transzparencia erősítése a mesterséges intelligencia alkalmazása során.[401]

Állami példamutatás

A védelmi szint következő fokának elérésében valamilyen módon mindig szerepe és felelőssége van az állami adatkezelőknek, illetve általában az államoknak. Olyan hatalom és gazdasági mozgástér koncentrálódik ugyanis náluk, ami egyetlen másik szereplővel sem hasonlítható össze. Az állami adatkezelők az adatkezeléseket megelőző döntéseik átláthatóságában példát mutathatnak a többi adatkezelőnek. Ennek kimondottan az adatvédelmi kultúrát építő, illetve erősítő jellege is van. Ne feledjük, az államnak ezen a téren is felelőssége van, nem csupán az adatvédelmi tisztviselőnek. Steven C. Bennett is érvel ezzel a felelősséggel, írásában a privát szférát erősítő megoldások használatában buzdítja kezdeményező szerepre az állami intézményeket.[402] Amennyiben ugyanis van kereslet egy bizonyos termékre, szolgáltatásra, úgy annak a piacra kedvező hatása van, ami végső soron a kedvezőbb védelem irányába mutat.

Az állam felelőssége különösen ott lehet jelentős, ahol a piac egyébként „természetes" módon éppen a gyengébb védelmet támogatja. Írásukban Balogh és szerzőtársai amellett szólnak, hogy gyakorlatilag egy ezzel ellentétes piaci logika nem ellenérv, hanem inkább érv az erőteljes és tudatos állami fellépés mellett.[403]

[401] Artificial Intelligence and Data Protection: Delivering Sustainable AI Accountability in Practice, Second Report: Hard Issues and Practical Solutions. *Huntonprivacyblog.com,* 2020. február 27–28.

[402] Steven C. Bennett: Government Options for Encouraging Use of Online Privacy-enhancing Technologies. *The Privacy Advisor, IAPP newsletter,* 11. (2011), 2. Forrás: a Jones Day honlapja.

[403] Balogh Zsolt et al.: Technológia a jog szolgálatában? Kísérletek az adatvédelem területén. *Pro Futuro,* 4. (2014), 1. 38.

A Rendelet kétéves alkalmazásának értékelése

Az elemzés lezárása előtt szót kell ejteni a Rendelet értékeléséről, amelyet az Európai Bizottság két évvel a Rendelet alkalmazandóvá válását követően volt köteles elvégezni.

A Bizottság értékelése alapvetően pozitív, sikeresnek tekinti a Rendelet alkalmazását, még akkor is, ha bizonyos kérdésekben elismeri a meglévő kihívásokat.

Kihívásokat lát még a hatóságok közötti együttműködésben, megemlítve (ahogyan arra én is kitértem) a tagállamok közötti eljárásjogi különbözőségeket, a hatóságok erőforráshiányát, a fragmentáció kockázatát vagy a változó technológiai környezetet. Elengedhetetlennek tartja annak biztosítását, hogy az EU adatvédelmi hatóságai szükség esetén hatékonyan léphessenek fel a nagy globális platformokkal szemben. A Bizottság a harmadik országok tekintetében a jövőre nézve is prioritásnak tekinti a megfelelő védelmi szintet megállapító határozatok ügyét.

A Bizottság megállapításaival és a kritikus pontokkal általában egyet lehet érteni, még akkor is, ha a saját értékelésem szerint az említett problémák mielőbbi megoldást sürgetnek, és a bizottsági értékelés már középtávon is konkrétabb lépéseket vehetne tervbe.

Az unió védelmi rendszere a harmadik országok viszonylatában különösen jelentős kérdéseket vet fel a 2020. július 16-i döntést követően. A fentebb már említett Schrems II ugyanis mintha némi zavart mutatna a döntéshozatalban. Az Európai Unió Bíróságának döntése egy olyan uniós jogalkotási aktust semmisített meg, amely egy harmadik ország, az Amerikai Egyesült Államok tekintetében állapította meg, hogy megfelelő védelmi szintet biztosít a személyes adatok védelme terén. Ez már a második olyan ítélet fél évtizeden belül, amely a nem megfelelő mérlegelés következményeként érvényteleníti a két kontinenst érintő jogi keretet.

Olvashatjuk ezt az ítéletet kritikusan is: mintha megerősítené azt a feladatunkat, hogy a saját védelmi rendszerünkkel kapcsolatos vizsgálatainkat végezzük el alaposan, mielőtt egy külsőt elemzünk, mert a Bizottság már másodszor tévedett jelentősen abban a tekintetben, hogy mi az a harmadik ország által nyújtott védelem, amely „lényegében megfelelő" *(essentially equivalent)* az unióéval összevetve. Szükséges annak tisztázása, hogy pontosan milyen védelmi pontokat várunk el a harmadik országok szereplőitől annak érdekében, hogy az unió jogában biztosított védelem valóban megőrizhető maradjon.

Zárszó

Minél erősebb és összetettebb kihívások érik az általunk elért védelmet, annál fontosabb a saját rendszerünk erősségeinek, valamint gyengéinek ismerete annak érdekében, hogy közös vívmányainkat megőrizhessük, és a védelem szintjét a jövőben ne csak megőrizni, hanem emelni is tudjuk.

Az adatvédelmi tisztviselők és az adatvédelmi felügyeleti hatóságok megerősített szerepe alkalmas lehet arra, hogy megteremtsék a védelem magasabb szintjét. Elemzésem ezt a célt szolgálta, ahogy a bevezetőben is említettem: a gyakorlatra fókuszáltam a munka során. Tisztában vagyok vele, hogy a levont következtetések és javaslatok adott esetben újszerűek vagy ambiciózusak. Egyet tudok érteni ezekkel a jelzőkkel, ha a piaci és kormányzati adatkezelők iránt teljes bizalommal fordulunk. Az adatpiac és az online manipuláció[404] jelenségével szembesülve azonban ez egy tökéletesen naiv hozzáállás lenne. Vagy a jogalkotó és a hatósági jogalkalmazás lép fel határozottan az érintetti, illetve fogyasztói jogokért, vagy továbbra is tétlenül követhetjük, ahogyan az online piac monopolizálódik, és ezzel párhuzamosan a demokráciák alapjait is megrengeti. Nem ezt az utat ajánlom. Giovanni Buttarelli figyelmeztetésével értek egyet, aki 2018 márciusában kiadott véleményében úgy fogalmazott: „nem elég a végső soron elszámoltathatatlan piaci szereplők jó szándékára alapozni".[405] Az elemzésben írt figyelmeztetés szellemében vontam le következtetéseimet.

Mi sem áll közelebb a szerző kívánságához, mint hogy az a magasabb szintű védelem, amelyről az előzőekben értekeztem, a polgáraink számára napi valósággá válhasson.

[404] A Cambridge Analytica-ügyről részletesen beszámol a brit Information Commissioner's Office (ICO) az Egyesült Királyság parlamentjének 2018. november 6-án kelt dokumentumában: Investigation into the Use of Data Analytics in Political Campaigns – A Report to Parliament. *Ico.org.uk,* 2018. november 6.

[405] European Data Protection Supervisor: Opinion on Online Manipulation and Personal Data. *Edps.europa.eu,* 2018. március 19. 23.

Felhasznált irodalom

Szakirodalom

Árvay Viktor – Balogh Gyöngyi – Buzás Péter – Eszteri Dániel – Hackspacher Andrea – Kiss Ernő – Majsa Ágnes – Révész Balázs: *Az új általános európai adatvédelmi szabályozás és az adatkezelői kötelezettségek.* Budapest, NKE, 2018. Online: http://hdl.handle.net/20.500.12944/7230

Asimov, Isaac: Körbe-körbe. In *Robottörténetek I.* Budapest, Móra Kiadó, 1993.

Balogh Zsolt – Kiss Attila – Polyák Gábor – Szádeczky Tamás – Szőke Gergely László: Technológia a jog szolgálatában? Kísérletek az adatvédelem területén. *Pro Futuro,* 4. (2014), 1. 33–45. Online: https://doi.org/10.26521/Profuturo/2014/1/5494

Bennett, Colin J. – Charles D. Raab: *The Governance of Privacy – Policy Instruments in Global Perspective*. London, The MIT Press, 2006. 133–143.

Bennett, Steven C.: Government Options for Encouraging Use of Online Privacy-Enhancing Technologies. *The Privacy Advisor, IAPP newsletter,* 11. (2011), 2. Online: https://bit.ly/3MFIvkk

Bentham, Jeremy: *Panopticon or the Inspection-House.* (h. n.), (k. n.), 1787.

Bloustein, Edward J.: Privacy as an Aspect of Human Dignity – An Answer to Dean Prosser. In Ferdinand D. Shoeman (szerk.): *Philosophical Dimension of Privacy – an Anthology.* Cambridge, Cambridge University Press, 1984. 156–202. Online: https://doi.org/10.1017/CBO9780511625138

Brandeis, Louis D. – Samuel D. Warren: The Right to Privacy. *Harvard Law Review,* 4. (1890), 5. 193–220. Online: https://bit.ly/3slsGYr

Carey, Peter: *Data Protection – A Practical Guide to UK and EU Law*. New York, Oxford University Press Inc., 2009.

Cavoukian, Ann: *Privacy by Design in Law, Policy and Practice – A White Paper for Regulators, Decision-makers and Policy-makers*. Ontario, Information and Privacy Commissioner, 2011.

Cukier, Kenneth – Viktor Mayer-Schoenberger: The Rise of Big Data – How It's Changing the Way We Think About the World. *Foreign Affairs,* 92. (2013), 3. 28–40. Online: https://bit.ly/3ynG0iA

Csepeli György: Veszélyesen élni? Avagy az internethasználat kockázatai. In Talyigás Judit (szerk.): *Az internet a kockázatok és mellékhatások tekintetében*. Budapest, Scolar Kiadó, 2010. 25–42.

Darcy, Allen – Alastair Berg – Chris Berg – Brendan Markey-Towlerand – Jason Potts: Some Economic Consequences of the GDPR. *Economics Bulletin,* 39. (2019), 2. 785–797. Online: https://bit.ly/3yobW6n

De Hert, Paul: Belgium, Courts, Privacy and Data Protection: An Inventory of Belgian Case Law From the Pre-GDPR Regime (1995–2015). *Brussels Privacy Hubworking Paper,* 15. (2019), 5.

De Hert, Paul – Dariusz Kloza – Paweł Makowski (szerk.): *Enforcing Privacy: Lessons from Current Implementations and Perspectives for the Future.* Warsaw, Wydawnictwo Sejmowe, 2015.
De Hert, Paul – Vagelis Papakonstantinou – Gianclaudio Malgieri – Laurent Beslay – Ignacio Sanchez: The Right to Data Portability in the GDPR: Towards User-centric Interoperability of Digital Services. *Computer Law & Security Review,* 34. (2018), 2. 193–203. Online: https://bit.ly/396gGmQ
Diakopoulos, Nicholas: *Algorithmic Accountability Reporting: on the Investigation of Black Boxes.* Colombia Journalism School – Tow Center for Digital Journalism, 2013. Online: https://bit.ly/3w6xfH2
Eszteri Dániel: Hogyan tanítsuk jogszerűen a mesterséges intelligenciánkat? *Magyar Jog,* 66. (2019), 12. 669–682.
Fairfield, Joshua A. T. – Christoph Engel: Privacy as a Public Good. *Duke Law Journal,* 65. (2015), 3. 385–457.
Ferry, W. H.: The Need for New Constitutional Controls. In Alan F. Westin (szerk.): *Information Technology in a Democracy.* Cambridge, Massachusetts, Harvard University Press, 2013. 207–213.
Foucault, Michel: *Discipline and Punish – The Birth of the Prison*. New York, Pantheon, 1977.
Foucault, Michel: *Felügyelet és büntetés. A börtön története.* Budapest, Gondolat Kiadó, 1990.
Gárdos-Orosz Fruzsina – Bedő Renáta: Az alapvető jogok érvényesítése a magánjogi jogviták során – az újabb alkotmánybírósági gyakorlat (2014–2018). *Alkotmánybírósági Szemle,* 1. (2018), 1. 3–15.
Gömbös Ervin: A számítástechnikai rendszerek titok-, vagyon- és tűzvédelme. *Számítástechnika,* 1981. március.
Gonçalves, Maria Eduarda: The EU Data Protection Reform and the Challenges of Big Data: Remaining Uncertainties and Ways Forward. *Information & Communications Technology Law,* 26. (2017), 2. 90–115. Online: https://bit.ly/38cB5Xb
Gutwirth, Serge – Yves Poullet – Paul De Hert – Cécile De Terwange – Sjaak Nouwt (szerk.): *Reinventing Data Protection?* Amsterdam, Springer, 2009, 135.
Hajdú József: Az innováció hatása a munkaerőpiacra, avagy elveszik-e a robotok az ember munkáját? *Forum: Acta Juridica et Politica,* 10. (2020), 2. 37–55. Online: http://acta.bibl.u-szeged.hu/70786/
Hijmans, Hielke: *The European Union as a Constitutional Guardian of Internet Privacy and Data Protection.* PhD-értekezés. Amszterdam, University of Amsterdam, 2016. Online: https://bit.ly/3KY2yZQ
Hustinx, Peter: The Role of Data Protection Authorities. In Serge Gutwirth – Yves Poullet – Paul De Hert – Cécile De Terwange – Sjaak Nouwt (szerk.): *Reinventing Data Protection?* Amsterdam, Springer, 2009. 131–143.
Jóri András: *Adatvédelmi kézikönyv.* Budapest, Osiris Kiadó, 2005.
Jóri András: Az információvédelemért és az információszabadságért felelős biztos intézményéről. *Fundamentum,* 14. (2010), 2. 20–29.
Jóri András: Shaping vs Applying Data Protection Law: Two Core Functions of Data Protection Authorities. *International Data Privacy Law,* 5. (2015), 2. 133–143.
Jóri András – Soós Andrea Klára – Bártfai Zsolt – Hári Anita: *A GDPR magyarázata*. Budapest, HVG-ORAC, 2018.

Klein Tamás – Tóth András (szerk.): *Technológia jog – Robotjog – Cyberjog*. Budapest, Wolters Kluwer Hungary Kft., 2018.
Kollár Csaba: A mesterséges intelligencia kapcsolata a humán biztonsággal. *Nemzetbiztonsági Szemle,* 6. (2018), 1. 5–23.
Krotoszynski, Ronald J., Jr.: *Privacy Revisited – A Global Perspective on the Right to Be Left Alone*. Oxford University Press, 2016.
Lasswell, Harold D.: Policy Problems of a Data-Rich Civilization. In Alan F. Westin (szerk.): *Information Technology in a Democracy*. Massachusetts, Harvard University Press, 1971. 187–197.
Le Métayer, Daniel: Privacy by Design: A Matter of Choice. In Serge Gutwirth – Yves Poullet – Paul De Hert (szerk.): *Data Protection in a Profiled World.* Amsterdam, Springer, 2010. 328–329.
Li, He – Lu Yu – Wu He: The Impact of GDPR on Global Technology Development. *Journal of Global Information Technology Management,* 22. (2019), 1. 1–6. Taylor & Francis Online, 2019. január 24. Online: https://bit.ly/3MYzXFb
Lynskey, Orla: The 'Europeanisation' of Data Protection Law. *Cambridge Yearbook of European Legal Studies*, 19. (2017). 252–286.
Lynskey, Orla: Grappling with "Data Power": Normative Nudges from Data Protection and Privacy. *Theoretical Inquiries in Law,* 20. (2019), 1. 189–220.
Majtényi László: *Az információs szabadságjogok – Adatvédelem és a közérdekű adatok nyilvánossága*. Budapest, Complex Kiadó, 2006.
McDonald, Aleecia M.: When Self-help helps: User Adoption of Privacy Technologies. In Marc Rothenberg – Julia Horwitz – Jeramie Scott (szerk.): *Privacy in the Modern Age – the Search for Solutions*. New York, The New Press, 2015.
Menyhárd Attila: A magánélethez való jog a szólás- és médiaszabadság tükrében. In Csehi Zoltán – Koltay András – Navratyil Zoltán (szerk.): *A személyiség és a média a polgári és a büntetőjogban – Az új Polgári Törvénykönyvre és az új Büntető Törvénykönyvre tekintettel*. Budapest, Wolters Kluwer Complex Kiadó, 2014.
Moore, Mark H.: *Creating Public Value: Strategic Management in Government*. Cambridge, Massachusetts, Harvard University Press, 1995.
Ottow, Annetje: *Market & Competition Authorities – Good Agency Principles*. Oxford University Press, 2015.
Péterfalvi Attila (szerk.): *Adatvédelem és információszabadság a mindennapokban*. Budapest, HVG ORAC, 2012.
Péterfalvi Attila – Szabó Endre Győző: Hol tart az Európai Unió adatvédelmi reformja? *Acta Humana,* 4. (2014), 2. 7–12.
Péterfalvi Attila – Révész Balázs – Buzás Péter: *Magyarázat a GDPR-ról*. Budapest, Wolters Kluwer Hungary, 2018.
Raab, Charles – Székely Iván: Data Protection Authorities and Information Technology. *Computer Law & Security Review,* 33. (2017), 4. 421–433. Online: https://bit.ly/3yoT5sa
Schneier, Bruce: Fear and Convenience. In Marc Rothenberg – Julia Horwith – Jeramie Scott (szerk.): *Privacy in the Modern Age – the Search for Solutions*. New York, The New Press, 2015.
Simitis, Spiros: Reviewing Privacy in an Information Society. *University of Pennsylvania Law Review,* 135. (1987), 3. 707–746.

Simon Éva: Az adatvédelmi hatásvizsgálat bevezetésének lehetősége. In Székely Iván – Szabó Máté Dániel (szerk.): *Szabad adatok, védett adatok*. Budapest, Információs Társadalomért Alapítvány, 2008.
Síthighand, Daithí Mac – Mathias Siems: The Chinese Social Credit System: A Model for other Countries? *EUI Working Papers,* (2019), 1.
Soós Andrea Klára: Az adatvédelmi hatóságok „teljes függetlensége": az Európai Unió Bíróságának gyakorlata. *Infokommunikáció és Jog,* (2012), 52–53. 219–223.
Sparrow, Malcolm K.: *The Character of Harms: Operational Challenges in Control*. New York, Harvard University Press, 2008.
Stalla-Bourdillon, Sophie – Alison Knight: Data Analytics and the GDPR: Friends or Foes? A Call for a Dynamic Approach to Data Protection Law. In R. Leenes – R. van Brakel – S. Gutwirth – Paul De Hert (szerk.): *Data Protection and Privacy: The Internet of Bodies Hart*. Oxford, Hart Publishing, 2018. 317–328. Online: https://bit.ly/3yjJiU9
Sulyok Tamás: *Az ügyvédi hivatás alkotmányjogi helyzete*. Szeged, Pólay Elemér Alapítvány, 2015.
Szabó Endre Győző: A SWIFT adatkezeléséről. *Jogi Fórum,* 2006. Online: https://bit.ly/3kQfpTx
Szabó Endre Győző: Méltóság és megfigyelés – Az emberi méltóság: érték és mérce. *Jogi Fórum,* 2009. július 13. Online: https://bit.ly/39N8sAm
Szabó Endre Győző: Személyes adat kezelése után fizetendő termékdíj – avagy osszuk meg a megosztott adatok hasznát! *Pázmány Law Working Papers,* (2014), 29. Online: http://plwp.eu/docs/wp/2014/2014-29_Szabo.pdf
Szabó Endre Győző: A kétoldalú piacok elmélete és a személyes adatok védelme – a Google-ítélet elemzése versenyjogi és adatvédelmi szempontok szerint. *In Medias Res,* 6. (2017), 1. 170–181.
Szabó Endre Győző: Adatvédelem és technológia. In Klein Tamás – Tóth András (szerk.): *Technológia jog – Robotjog – Cyberjog.* Budapest, Wolters Kluwer, 2018. 26–86.
Szabó Endre Győző: Az adatvédelmi tisztviselőről – a GDPR szabályainak elemzése. *Infokommunikáció és Jog,* 70. (2018), 1. 3–10. Online: https://bit.ly/3vTDOh8
Szabó Máté Dániel: *Az információs hatalom alkotmányos korlátai*. Miskolc, Miskolci Egyetem, 2012.
Székely Iván: Kukkoló társadalom – avagy van-e még függöny virtuális ablakunkon. In Talyigás Judit (szerk.): *Az internet a kockázatok és mellékhatások tekintetében.* Budapest, Scolar Kiadó, 2010. 93–20.
Szilágyi Péter: Jogbölcseleti mozaikok a jog hatékonysága kapcsán. In Nochta Tibor – Monori Gábor (szerk.): *Ius Est Ars. Ünnepi tanulmányok Visegrády Antal professzor 65. születésnapja tiszteletére.* Pécs, PTE ÁJK, 2015. 471–474.
Szőke Gergely László: Az adatvédelem szabályozásának történeti áttekintése. *Infokommunikáció és Jog,* 56. (2013), 3. 107–112.
Szőke Gergely László: Big Data and Algorithms in the Public Sector and their Impact on the Transparency of Decision-making. In *Central and Eastern European e|Dem and e|Gov Days 2018*. Bécs, Austrian Computer Society, 2018. 301–311. Online: https://bit.ly/3KXcMKj
Talyigás Judit (szerk.): *Az internet a kockázatok és mellékhatások tekintetében*. Budapest, Scolar Kiadó, 2010.

Van Alsenoy, Brendan – Valerie Verdoodt – Rob Heyman – Jef Ausloos – Ellen Wauters – Güneş Acar: From Social Media Service to Advertising Network. A Critical Analysis of Facebook's Revised Policies and Terms. *Researchgate.net*, 2015. augusztus 25. Online: https://bit.ly/3kYt8HH

Váradi Szilvia: A közszférára vonatkozó adatvédelmi szabályok a GDPR tükrében. *Pro Futuro,* 9. (2019), 1. 39–54. Online: https://bit.ly/3kQeW3J

Váradi Szilvia – Kertész Attila – Michael Parkin: The Necessity of Legally Compliant Data Management in European Cloud Architectures. *Computer Law & Security Review,* 28. (2012), 5. 577–586.

Várkonyi, Gizem Gültekin – Váradi Szilvia – Kertész Attila: Legal Aspects of Operating IoT Applications in the Fog. In Buyya Rajkumar – Satish Narayana Srirama (szerk.): *Fog and Edge Computing: Principles and Paradigms*. Hoboken, John Wiley & Sons, 2019. 411–432.

Visegrády Antal: A jogi kultúra és a joghatékonyság keretei. *JURA,* 23. (2017), 2. 238–254.

Westin, Alan F. (szerk.): *Information Technology in a Democracy*. Cambridge, Massachusetts, Harvard University Press, 1971.

Westin, Alan: The Origins of Modern Claims to Privacy. In Ferdinand D. Shoeman (szerk.): *Philosophical dimensions of privacy. An anthology*. Cambridge, Cambridge University Press, 1984. 56–74.

Zarsky, Tal: Incompatible: The GDPR in the Age of Big Data. *Seton Hall Law Review,* 47. (2017), 4(2). 995–1020. Online: https://bit.ly/3wdLpX1

Zarsky, Tal: Privacy and Manipulation in the Digital Age. *Theoretical Inquiries in Law,* 20. (2019), 1. 157–188.

Ződi Zsolt: Privacy és a Big Data. *Fundamentum,* 21. (2017), 1–2. 18–30.

Intézményi dokumentumok

28. Tätigkeitsbericht Datenschutz des Hamburgischen Beauftragten für Datenschutz und Informationsfreiheit 2019, 93–95. Online: https://bit.ly/3LYESGg

A Gazdasági Versenyhivatal elnökének és a Gazdasági Versenyhivatal Versenytanácsa elnökének 11/2017. közleménye a versenykorlátozó megállapodásokra és összehangolt magatartásokra, a gazdasági erőfölénnyel való visszaélésre, valamint a jelentős piaci erővel való visszaélésre vonatkozó tilalmakba ütköző magatartások esetén a bírság összegének megállapításáról. Online: https://bit.ly/3MWkjdy

A Gazdasági Versenyhivatal elnökének és a Gazdasági Versenyhivatal Versenytanácsa elnökének 12/2017. közleménye a fogyasztóvédelmi típusú ügyekben kiszabott bírság meghatározásának szempontjairól Online: https://bit.ly/3P7srJZ

A bajor adatvédelmi biztos közleménye: *„Pressemitteilung: Datenschutzbeauftragter darf keinen Interressenkonflikten unterliegen".* Ansbach, 2016. október 20. Online: https://bit.ly/3kRMs9H

Contribution of the EDPB to the evaluation of the GDPR under Article 97, elfogadva: 2020. február 18-án. Online: https://bit.ly/3MR3osW

DPO Network: *Professional Standards for Data Protection Officers of the EU Institutions and Bodies Working under Regulation (EC) 45/2001,* 2010. október 14. Online: https://bit.ly/3ykrqbB

ENSZ Közgyűlése: 68/167. számú határozata*: A magánélethez való jog a digitális korban* (Resolution No. 68/167 Adopted by the General Assembly on the Right to Privacy in the Digital Age), 2013. december 18. Online: https://bit.ly/39G2npb

ENSZ 2014. január 21-i közleménye: *The Right to Privacy in the Digital Age.* Online: https://bit.ly/3N10GRD

Az európai adatvédelmi biztos előzetes véleménye az adatvédelemről és a versenyképességről az óriás méretű adathalmazok korában, 2014. március 26. Online: https://bit.ly/3vXavKS

Az európai adatvédelmi biztos stratégiája, 2015–2019. (Leading by example – The EDPS Strategy 2015–2019, 3.) Online: https://bit.ly/3kVFJM1

Az európai adatvédelmi biztos 3/2018. számú véleménye az online manipulációról és a személyes adatokról, 2018. március 19. Online: https://bit.ly/3kQK8j9

Európai Adatvédelmi Testület 2/2018. sz. iránymutatása az (EU) 2016/679 rendelet 49. cikke szerinti eltérésekről, elfogadás időpontja: 2018. május 25.

Európai Unió Alapjogi Ügynöksége: *Data Protection in the European Union: the Role of National Data Protection Authorities – Strengthening the Fundamental Rights Architecture in the EU II.* Luxembourg, Publications Office of the European Union, 2010. Online: https://bit.ly/3FqlOhG

Európa Tanács: *Explanatory Report to the Additional Protocol to the Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data, Regarding Supervisory Authorities and Transborder Data Flows.* Strasbourg, 2001. november 8.

Európai Unió Alapjogi Ügynöksége és az Európa Tanács: Európai adatvédelmi jogi kézikönyv – 2018. évi kiadás. Az Európai Unió Kiadóhivatala, Luxemburg, 2019. Online: https://bit.ly/3P7D3bP

Európai Unió Tanácsa: *Council Conclusions on the Communication from the Commission to the European Parliament and the Council – A Comprehensive Approach on Personal Data Protection in the European Union.* Brüsszel, 2011. február 24–25. Online: https://bit.ly/3ypXefk

European Union Agency for Fundamental Rights and Council of Europe: Handbook on European Law Relating to Access to Justice, 2016. Online: https://bit.ly/3P0uuQh

Monteleone, Shara – Laura Piccio: *From Safe Harbor to Privacy Shield – Advances and Shortcomings of the New EU-US Data Transfer Rules.* European Parliament Research Service, 2017. Online: https://bit.ly/3waTWtO

NAIH tájékoztató az adatvédelmi tisztviselők képzésével kapcsolatban. 2018. április 24. Online: www.naih.hu/files/2018-04-24-DPO-edu.pdf

Special Eurobarometer 359: *Attitudes on Data Protection and Electronic Identity in the European Union,* 2011. Online: https://bit.ly/3vXHY80

Special Eurobarometer 431: *Adatvédelem,* 2015. Online: https://bit.ly/3FtxS1t

Special Eurobarometer 487a: *Az általános adatvédelmi rendelet,* 2019. Online: https://bit.ly/3snZlMZ

Egyéb forrás

Az IAPP (International Association of Privacy Professionals): GDPR Conundrums: The Data Protection Officer Requirement. *Research.tilburguniversity.edu*, 2016. július 19. Online: https://bit.ly/3sikGan

Maraniss, David – Michael Weisskopf: OSHA'S Enemies Find themselves in High Places. *The Washington Post*, 1995. július 24. Online: https://wapo.st/3MTcCou/

Moerel, L.: GDPR Conundrums – The Data Protection Officer Requirement. *Iapp.org*, 2016. júliuis 19. Online: https://bit.ly/3w8guLE

Pozen, E. David: Edward Snowden, National Security Whistleblowing, and Civil Disobedience. *Columbia Law School*, 2019. Online: https://bit.ly/38X6VHi

The GDPR Demands 75k DPOs – Where Will They Come From? *Iapp.org.* Online: https://bit.ly/3KQi61K

A 29. cikk szerinti adatvédelmi munkacsoport munkássága – időrendi sorrendben

A 29. cikk szerinti adatvédelmi munkacsoport: *04/2007 sz. vélemény a személyes adat fogalmáról, WP136*, elfogadás időpontja: 2007. június 20. Online: https://bit.ly/3OZIqd7

A 29. cikk szerinti adatvédelmi munkacsoport: *3/2010 sz. vélemény az elszámoltathatóság elvéről, WP173*, elfogadás időpontja: 2010. július 13. Online: https://bit.ly/3LRrnrT

A 29. cikk szerinti adatvédelmi munkacsoport: *2012/1. sz. vélemény az adatvédelmi reformjavaslatokról, WP191*, elfogadás időpontja: 2012. március 23. Online: https://bit.ly/39AjjNL

A 29. cikk szerinti adatvédelmi munkacsoport: *03/2014 sz. vélemény személyes adatok megsértése bejelentéséről, WP213*, elfogadás időpontja: 2014. március 25. Online: https://bit.ly/3l3Vsc5

A 29. cikk szerinti adatvédelmi munkacsoport: *Iránymutatás az EUB „Google Spain and Inc kontra Agencia Española de Protección de Datos (AEPD) és Mario Costeja González" C-131/12. sz. ügyben hozott ítéletének végrehajtására vonatkozóan, WP225*, elfogadás időpontja: 2014. november 26. Online: https://bit.ly/3yjhcrW

A 29. cikk szerinti adatvédelmi munkacsoport közleménye: *Statement on the Implementation of the Judgement of the Court of Justice of the European Union of 6 October 2015 in the Maximilian Schrems v Data Protection Commissioner case (C-362-14)*, 2015. október 16. Online: https://bit.ly/39HG3f0

A 29. cikk szerinti adatvédelmi munkacsoport: *Iránymutatás az adatok hordozhatóságáról, WP242*, elfogadás időpontja: 2016. december 13., felülvizsgálva 2017. április 5-én. Online: https://bit.ly/3kRIT37

A 29. cikk szerinti adatvédelmi munkacsoport: *Iránymutatás az adatvédelmi tisztviselőkkel kapcsolatban, WP243 rev.01*, elfogadás időpontja: 2016. december 13., felülvizsgálva 2017. április 5-én. Online: https://bit.ly/3MVMfOJ

A 29. cikk szerinti adatvédelmi munkacsoport: *Iránymutatása az adatvédelmi hatásvizsgálat elvégzéséhez és annak megállapításához, hogy az adatkezelés az (EU) 2016/679 rendelet*

alkalmazásában „valószínűsíthetően magas kockázattal jár-e", WP248rev.01, az elfogadás időpontja: 2017. április 4. Online: https://bit.ly/3w7mh3V

A 29. cikk szerinti adatvédelmi munkacsoport*: Iránymutatás a 2016/679 rendelet szerinti közigazgatási bírság alkalmazásáról és megállapításáról, WP253,* elfogadás időpontja: 2017. október 3. Online: https://bit.ly/3KT7HT0

A 29. cikk szerinti adatvédelmi munkacsoport: *Iránymutatás az (EU) 2016/679 rendelet szerinti hozzájárulásról, WP259 rev. 01,* az elfogadás időpontja: 2017. november 28., utolsó felülvizsgálat: 2018. április 10-én. Online: https://bit.ly/3LSv9Bk

Az Európai Bizottság dokumentumai – időrendi sorrendben

A Bizottság közleménye az Európai Parlamentnek, a Tanácsnak és az Európai Gazdasági és Szociális Bizottságnak: *A magánélet védelme az összekapcsolódó világban – 21. századi európai adatvédelmi keret.* Brüsszel, COM(2012)09, végleges: 2012. január 25. Online: https://bit.ly/3ymLHNN

Az Európai Bizottság 26. számú véleménye: *Az információs és kommunikációs technológiák etikájáról (Opinion No. 26, Ethics of Information and Communication Technologies).* Brüsszel, 2012. február 22. Online: https://bit.ly/37ke1Fs

A Bizottság közleménye az Európai Parlamentnek és a Tanácsnak: *A 95/46/EK irányelv alapján, az Európai Bíróság C-362/14. sz. (Schrems-)ügyben hozott ítéletét követően a személyes adatoknak az Európai Unióból az Amerikai Egyesült Államokba történő továbbításáról.* Brüsszel, COM(2015)566, végleges: 2015. november 6. Online: https://bit.ly/39Ln4jP

A Bizottság közleménye az Európai Parlamentnek és a Tanácsnak: *Erősebb védelem, új lehetőségek – a Bizottság iránymutatása az általános adatvédelmi rendelet 2018. május 25-től történő közvetlen alkalmazásáról.* Brüsszel, COM(2018)043, végleges: 2018. január 24. Online: https://bit.ly/390emhb

A Bizottság közleménye az Európai Parlamentnek, a Tanácsnak, az Európai Gazdasági és Szociális Bizottságnak és a Régiók Bizottságának: *Európa digitális jövőjének megtervezése.* Brüsszel, COM(2020)67, végleges: 2020. február 19. Online: https://bit.ly/37kdxz8

A Bizottság közleménye az Európai Parlamentnek, a Tanácsnak, az Európai Gazdasági és Szociális Bizottságnak és a Régiók Bizottságának: *Európai adatstratégia.* Brüsszel, COM(2020)66, végleges: 2020. február 19. Online: https://bit.ly/3kM1ayU

Európai Bizottság: *Fehér könyv a mesterséges intelligenciáról: a kiválóság és a bizalom európai megközelítése.* Brüsszel, COM(2020)65, végleges: 2020. február 19. Online: https://bit.ly/3kNRJiG

A Bizottság közleménye az Európai Parlamentnek és a Tanácsnak: *A polgárok szerepe erősítésének és az EU digitális átállással kapcsolatos megközelítésének pillérét képező adatvédelem – az általános adatvédelmi rendelet alkalmazásának két éve.* COM/(2020)264, végleges: 2020. június 24. Online: https://bit.ly/3sfyzpQ

Commission Staff Working Document, Accompanying the Document: *Communication from the Commission to the European Parliament and the Council, Data Protection as a Pillar of Citizen's Empowerment and the EU's Approach to the Digital Transition – Two Years of Application of the General Data Protection Regulation.* SWD(2020)115 final. Online: https://bit.ly/3P3Y8nN

Internetes források

A holland adatvédelmi hatósághoz érkező állampolgári megkeresések tárgyában született dokumentum; a dokumentum a holland adatvédelmi hatóság honlapján olvasható. *Autoriteitpersoonsgegevens.nl,* 2018. május 25. Online: https://bit.ly/3shrk0I

A holland adatvédelmiincidens-bejelentési kötelezettségről; a dokumentum a holland adatvédelmi hatóság honlapján olvasható. *Autoriteitpersoonsgegevens.nl,* 2015. december 8. Online: https://bit.ly/3wbshJ9

A Kodak 1888-ban piacra került fényképezőgépéről. *Americanhistory.si.edu.* Online: https://s.si.edu/3vNJd9o

A Rendelet 35. cikk (4) bekezdése szerinti a NAIH által nyilvánosságra hozott hatásvizsgálati lista. *Naih.hu.* Online: https://bit.ly/3wcaMIq

Artificial Intelligence and Data Protection: Delivering Sustainable AI Accountability in Practice, Second Report: Hard Issues and Practical Solutions. *Huntonprivcyblog.com,* 2020. február. 27–28. Online: https://bit.ly/3ykz5XG

Az International Conference of Information Commissioners (ICIC) honlapja. *Informationcommissioners.org.* Online: https://bit.ly/3w65w9r

Eric Schmidtnek, a Google vezérigazgatójának a CNBC számára adott interjúja, melyről az Electronic Frontier Foundation a honlapján számol be. *Eff.org,* 2009. december 10. Online: https://bit.ly/3sc4UOr

Investigation into the Use of Data Analytics in Political Campaigns – A report to Parliament. *Ico.org.uk,* 2018. november 18. Online: https://bit.ly/3Fm6H8U

Johnson, Bobbie: Privacy No Longer a Social Norm, Says Facebook Founder. *The Guardian,* 2010. január 11.

Hivatkozott magyar bírósági ítéletek

A Fővárosi Közigazgatási és Munkaügyi Bíróság 13.K.32.819/2015/16. számú ítélete

A Fővárosi Közigazgatási és Munkaügyi Bíróság 29.K.34.567/2015/16. számú ítélete

A Fővárosi Törvényszék 2.K.31.506/2018/8. számú ügyben hozott ítélete

A Fővárosi Törvényszék 13.K.700.014/2018/60. számú ügyben hozott ítélete

A Kúria Kfv.III.37.911/2017/8. számú ügyben hozott ítélete

Hivatkozott egyéb ítéletek

A német szövetségi alkotmánybíróság 1983-as Volkszählung ítélete – Urteil des Bundesverfassungsgerichts vom 15. Dezember 1983, 1 BvR 209/83, 1 BvR

A Nemzeti Adatvédelmi és Információszabadság Hatóság ügyei

NAIH/2017/148-as számú ügy
NAIH/2018/5457-es számú ügy
NAIH/2018/6093-as számú ügy
NAIH/2018/6142-es számú ügy
NAIH/2018/7142-es számú ügy
NAIH/2018/7235-ös számú ügy
NAIH/2019/55-ös számú ügy
NAIH/2019/167-es számú ügy
NAIH/2019/596-os számú ügy
NAIH/2019/1598-as számú ügy
NAIH/2019/1841-es számú ügy
NAIH/2019/1859-es számú ügy
NAIH/2019/2076-os számú ügy
NAIH/2019/2471-es számú ügy
NAIH/2019/2485-ös számú ügy
NAIH/2019/2466-os számú ügy
NAIH/2019/2472-es számú ügy
NAIH/2019/2668-as számú ügy
NAIH/2019/3114/8 számú ügy
NAIH/2019/3854-es számú ügy
NAIH/2020/1160-os számú ügy

Az Emberi Jogok Európai Bíróságának hivatkozott ítéletei

EJEB, Amann kontra Svájc [GC], 27798/95 számú ítélet, ECHR 2000 II; ECLI:CE:ECHR:2000:0216JUD002779895

EJEB, Bărbulescu kontra Románia [GC], 2017. szeptember 5-én kelt 61496/08 számú ítélet; ECLI:CE:ECHR:2016:0112JUD006149608

EJEB, Biriuk kontra Litvánia, 2008. november 25-én kelt 23373/03 számú ítélet; ECLI:CE:ECHR:2008:1125JUD002337303

EJEB, Fernández Martínez kontra Spanyolország [GC], 56030/07 számú ítélet, ECHR 2014-II; ECLI:CE:ECHR:2014:0612JUD005603007

EJEB, Halford kontra Egyesült Királyság, 1997 június 25-én kelt ítélet, ECLI:CE:ECHR:1997:0625JUD002060592

EJEB, Klass és mások kontra Németország, 1978. szeptember 6-án kelt ítélet, ECLI:CE:ECHR:1978:0906JUD000502971

EJEB, K.U. kontra Finnország, 2872/02 számú ítélet, ECHR 2008-V; ECLI:CE:ECHR:2008:1202JUD000287202

EJEB, López Ribalda és mások kontra Spanyolország [GC], 2019. október 17-én kelt 1874/13 és 8567/13 számú ítéletek; ECLI:CE:ECHR:2019:1017JUD000187413

EJEB, Petrenco kontra Moldávia, 2010. március 30-án kelt 20928/05 számú ítélet; ECLI:CE:ECHR:2010:0330JUD002092805
EJEB, Rotaru kontra Románia [GC], 28341/95 számú ítélet, ECHR 2000-V; ECLI:CE:ECHR:2000:0504JUD002834195
EJEB, S. és Marper kontra Egyesült Királyság [GC], 30562/04 és 30566/04 számú ítéletek; ECHR 2008-V; ECLI:CE:ECHR:2008:1204JUD003056204
EJEB, Sciacca kontra Olaszország, 50774/99 számú ítélet, ECHR 2005-I; ECLI:CE:ECHR:2005:0111JUD005077499
EJEB, Söderman kontra Svédország [GC], 5786/08 számú ítélet, ECHR 2013-VI; ECLI:CE:ECHR:2013:1112JUD000578608
EJEB, Szabó és Vissy kontra Magyarország, 2016. január 12-én kelt 37138/14 számú ítélet; ECLI:CE:ECHR:2016:0112JUD003713814
EJEB, Von Hannover kontra Németország, 59320/00 számú ítélet, ECHR 2004-VI; ECLI:CE:ECHR:2004:0624JUD005932000
EJEB, Von Hannover kontra Németország (no. 2) [GC], 40660/08 és 60641/08 számú ítéletek, ECHR 2012-I; ECLI:CE:ECHR:2012:0207JUD004066008
EJEB, Z kontra Finnország, 1997. február 25-én kelt ítélet, Jelentések 1997-I; ECLI:CE:ECHR:1997:0225JUD002200993

Az Európai Unió Bíróságának hivatkozott ítéletei

EUB, Európai Bizottság kontra Ausztria [nagytanács], C-614/10. sz. ügy, 2012. ECLI:EU:C:2012:631
EUB, Európai Bizottság kontra Magyarország [nagytanács], C-288/12. sz. ügy, 2014. ECLI:EU:C:2014:237
EUB, Európai Bizottság kontra Német Szövetségi Köztársaság [nagytanács], C-518/07. sz. ügy, 2010. ECLI:EU:C:2010:125
EUB, Digital Rights Ireland és Kärntner Landesregierung és társai [nagytanács], C-293/12 és C-594/12 sz. egyesített ügyek, 2014. ECLI:EU:C:2014:238
EUB, Fashion ID GmbH & Co.KG kontra Verbraucherzentrale NRW eV, C-40/17. sz. ügy, 2019. ECLI:EU:C:2019:629
EUB, František Ryneš kontra Úřad pro ochranu osobních údajů, C-212/13. sz. ügy, 2014. ECLI:EU:C:2014:2428
EUB, Google Spain SL és Google Inc. kontra Agencia Española de Protección de Datos (AEPD) és Mario Costeja González [nagytanács], C-131/12. sz. ügy, 2014. május 13. ECLI:EU:C:2014:317
EUB, Klaus Höfner és Fritz Elser kontra Macrotron GmbH, C-41/90. sz. ügy, 1991. ECLI:EU:C:1991:161
EUB, Bodil Lindqvist kontra Svédország, C-101/01.sz. ügy, 2004. ECLI:EU:C:2003:596
EUB, Maximillian Schrems kontra adatvédelmi biztos [nagytanács], C-362/14 sz. ügy, 2015. ECLI:EU:C:1991:161
EUB, Data Protection Commissioner kontra Facebook Ireland Ltd, Maximillian Schrems Az Európai Unió Bíróságának ítélete, C-311/18. sz. ügy, 2020. ECLI:EU:C:2020:559

Hivatkozott jogszabályok, egyezmények

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

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

Az Európai Parlament és a Tanács 45/2001/EK Rendelete (2000. december 18.) a személyes adatok közösségi intézmények és szervek által történő feldolgozása tekintetében az egyének védelméről, valamint az ilyen adatok szabad áramlásáról

Az Európai Parlament és a Tanács 585/2014/EU határozata (2014. május 15.) az Európai Unió egészére kiterjedő, kölcsönösen átjárható e-segélyhívó szolgáltatás kiépítéséről

Az Európai Parlament és a Tanács 95/46/EK irányelve (1995. október 24.) a személyes adatok feldolgozása vonatkozásában az egyének védelméről és az ilyen adatok szabad áramlásáról

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

Az Európa Tanácsnak az egyének védelméről a személyes adatok gépi feldolgozása során, Strasbourgban, 1981. január 28. napján kelt Egyezménye (az úgynevezett 108-as egyezmény)

Additional Protocol to the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, regarding supervisory authorities and transborder data flows (ETS No. 181)

Az Európai Unió Alapjogi chartája (2012/C 326/02)

Az Európai Unióról szóló szerződés és az Európai Unió működéséről szóló szerződés egységes szerkezetbe foglalt változata (2012/C 326/01)

Magyarország Alaptörvénye (2011. április 25.)

Emberi jogok egyetemes nyilatkozata

1992. évi LXIII. törvény a személyes adatok védelméről és a közérdekű adatok nyilvánosságáról

1997. évi XLVII. törvény az egészségügyi és a hozzájuk kapcsolódó személyes adatok kezeléséről és védelméről

1998. évi VI. törvény az egyének védelméről a személyes adatok gépi feldolgozása során, Strasbourgban, 1981. január 28. napján kelt Egyezmény kihirdetéséről

2004. évi XXXIV. törvény a kis- és középvállalkozásokról, fejlődésük támogatásáról

2005. évi CXXXIII. törvény a személy- és vagyonvédelmi, valamint a magánnyomozói tevékenység szabályairól

2011. évi CXII. törvény az információs önrendelkezési jogról és az információszabadságról

Szabó Endre Győző jogász, a Nemzeti Adatvédelmi és Információszabadság Hatóság elnökhelyettese, az Európai Adatvédelmi Testületben a Cooperation szakértői alcsoport vezetője. Az adatvédelem nemzetközileg is ismert és elismert szakértője, a privacy jogának kutatója.

Az Európai Unió általános adatvédelmi rendelete, a 2018 májusától alkalmazandó GDPR a magánélet védelmének ünnepelt és világszerte ismert jogszabálya.

Az unió tagállamai büszkék arra, hogy a többi szabályozási megoldással összehasonlítva itt érvényesül a legmagasabb szintű védelem.

De vajon mi alapján tudjuk összehasonlítani a különböző védelmi szinteket és az ezek mögött álló szabályozások minőségét? Mi teszi a védelmet erőssé vagy éppen gyengévé? Milyen szempontok segítenek annak megítélésében, hogy előrelépés vagy éppen visszalépés történt?

A kötet ezekre a kérdésekre keres és ad választ az adatvédelmi gondolkodásban újszerűen ható védelmi lépcső elméletével. Egyszerű, de mégis szemléletes kísérlet a védelem minőségének és szintjének mérésére, amely a jogi szabályozás jövőbeni lehetséges fejlesztésének távlatát is megnyitja.