

Szabó Endre Győző

# A védelmi lépcső elmélete



**LUDOVIKA**  
EGYETEMI KIADÓ



Vákát

Szabó Endre Győző

# A védelmi lépcső elmélete

A GDPR védelmi szintjének elemzése



**LUDOVIKA**  
EGYETEMI KIADÓ  
Budapest, 2022

Szakmai lektor:  
Váradai 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: [kiadvanyok@uni-nke.hu](mailto:kiadvanyok@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

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

© A szerző, 2022  
© Ludovika Egyetemi Kiadó, 2022

Minden jog védve.

*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

Előszó	13
A szerző előszava	15
Bevezetés	17
A védelem szükségességéről	20
A védelmi szint kérdéseinek vizsgálata	27
Módszertani, értelmezési és rendszertani kérdések	28
A kutatás módszere	28
A nyelvtani értelmezés	28
A normacél szerinti (teleologikus) értelmezés	29
Az Európa-konform jogértelmezés	29
Rendszertani kérdések	30
A védendő jog és a védelem szintjének kérdései a személyes adatok vonatkozásában	31
A magánszféra fogalmának születése: a magánszféra és a technológia összefüggései	31
A magánszférához fűződő jog	38
A Rendeletben védett jog tartalma és terjedelme az emberi jogok európai egyezményének fényében	41
A védelem szintjének kérdései az Európai Unió Alapjogi chartájában	41
A magánélet fogalmának meghatározása az Emberi Jogok Európai Bíróságának esetjogában	43
Egyezmények által biztosított jogi keret	43
A magánélet fogalma	45
Személyes adatok kezelése – beavatkozás a magánélethez fűződő jogba	47
Az állam pozitív és negatív kötelezettségeiről	49
A személyes adatok védelméhez fűződő jog – a horizontális jogvédelem kérdései	50
A védendő jog mibenléte a Rendelet alapján	53
A Rendelet értelmezési kerete	53
A Rendelet elemzésének kiindulópontjai	57
A Rendelet áttekintő elemzése	59



A védelem komponensei és a védelem szintjének kérdései a Rendelet szabályozásában – a védelmi lépcső elmélete	61
A kontextus	61
Az adatvédelmi jog generációi	61
A védelem komponensei és fokozatai	62
A védelmi lépcső fokozatainak azonosítása	63
Az előrelépés lehetőségei a védelmi lépcsőn	64
Az állam kiemelt felelőssége	67
A normakövetés és az adatvédelmi kultúra összefüggései	67
Az adatvédelmi jog hatékonysága	68
Az adatvédelmi hatóságok hatékony működése	70
A védelem komponensei – a védelmi lépcső révén mérhető indikátorok általános elemzése	73
A Rendelet hatálya	73
Tárgyi hatály	74
Területi hatály	77
Személyi hatály	78
Definíciók	81
Átláthatóság	82
Az érintettek jogai	84
A központi adatvédelmi nyilvántartások megszűnése, belső nyilvántartások vezetése	86
Adatvédelmi hatásvizsgálat	87
Az adatvédelmi tisztviselő	88
A harmadik országba irányuló adattovábbítások szabályainak egységesítése	89
Független adatvédelmi felügyeleti hatóságok	91
Adatvédelmi felügyeleti hatóságok együttműködése határon átnyúló adatkezelés esetén	92
Az adatvédelmi incidensek bejelentésének kötelezettsége	93
Adatvédelmi bírság	95
Az adatvédelmi szabályozás technológiai fejlődést és változó üzleti modelleket követő rendszeres felülvizsgálata	96
Összegzés	98
A Rendelet egyes jogintézményeinek részletes elemzése – az adatvédelmi tisztviselő	101
Az adatvédelmi tisztviselői intézmény	102
Kockázatok és elszámoltathatóság	103
Az adatvédelmi tisztviselők szerepe	104

Előrelépés a védelmi lépcsőn és az adatvédelmi tisztviselői intézmény léte	106
Az adatvédelmi tisztviselő kinevezésének kötelezettsége	108
Értelmezési kérdések	111
Fő tevékenység	111
Nagymértékű adatkezelés	112
Rendszeres és szisztematikus megfigyelés	112
Az adatkezelőnek vagy az adatfeldolgozónak kell kineveznie az adatvédelmi tisztviselőt?	113
A kinevezési kötelezettség köre a védelmi lépcső fényében	114
Az adatvédelmi tisztviselő feladatai és jogállása	115
A foglalkoztatás szabályai	117
A tisztviselő adatainak nyilvánossága, elérhetőség	118
Teljes vagy részmunkaidős foglalkoztatás	118
Az adatkezelő feladatai a tisztviselő munkájának támogatása terén	119
Összeférhetetlenség	122
Az adatvédelmi tisztviselő feladatai – tanácsadás, ellenőrzés, kapcsolattartás	123
A tisztviselő feladatai az adatvédelmi hatásvizsgálat kapcsán	124
Összegzés	125
Az adatvédelmi tisztviselő feladatai és jogállása a védelmi lépcső elméletének fényében	125
A Rendelet egyes jogintézményeinek részletes elemzése – az adatvédelmi felügyeleti hatóságok	131
A felügyeleti hatóságok szerepe	132
Az adatvédelmi hatóságok létrehozásának szükségességéről	134
Az adatvédelmi felügyeleti hatóságok létrehozatala a védelmi lépcső elméletének fényében	137
A hatóságok feladatai – a védelem erősítésének és egységesítésének eszközei	137
Általános feladatok	138
A köz és az érintettek irányába mutató feladatok	138
A hatóságok belső feladatai	139
A jogalkotási és közigazgatási tervezetek véleményezése	139
Együttműködés más felügyeleti hatóságokkal és az Európai Adatvédelmi Testület munkájában való részvétel	140
Az adatkezelőkkel és adatfeldolgozókkal összefüggő feladatok	140
A külföldre irányuló adattovábbítással összefüggő feladatok	141
További, tagállami szinten meghatározott feladatok	141
Ingyenesség	142

A felügyeleti hatóságok feladatai a védelmi lépcső és a jog hatékonyságának fényében	143
Egységes feladatkör	143
A feladatok bővülésének mennyiségi és minőségi kérdései	143
A hatóságok új szemléletű feladatellátása	147
A panaszokat megelőző stratégia	149
A felügyeleti hatóságok hatásköre	154
Vizsgálati hatáskörök	155
Korrekciós hatáskörök	156
Az adatvédelmi hatóságok eljárásaival szemben támasztott uniós jogi követelmények	163
A tagállami adatvédelmi felügyeleti hatóságok hatásköre a védelmi lépcső fényében	165
Az adatvédelmi bírság	168
Magas védelmi szint biztosítása a tagállamokban – az adatvédelmi bírság intézménye a védelmi lépcső fényében	170
A bírság kiszabásának mérlegelése	172
A bírság kiszabásának szempontjai és a védelmi lépcső alkalmazása	172
A jogsértés jellege, súlyossága, időtartama	173
A kár mértéke	174
A kár enyhítése érdekében tett intézkedések	175
Az érintettek száma	176
A jogsértés szándékos vagy gondatlan jellege	177
A felelősség mértéke	178
Korábbi releváns jogsértések	179
Korábbi hatósági intézkedések ugyanabban a tárgyban	179
A tudomásszerzés módja	180
A jogsértéssel érintett adatkategóriák	182
A magatartási kódex és a tanúsítás szerepe a bírságkiszabás során	184
Egyéb körülmények	185
A bírsággal szemben támasztott általános elvárások	188
A bírság mértéke	189
Enyhébb megítélésű jogsértések	189
Súlyosabb jogsértések	191
A felügyeleti hatóság utasításának figyelmen kívül hagyása	192
A bírság legalacsonyabb és legmagasabb összege	192
Az előrelépés lehetősége a védelmi lépcsőn a bírság összege terén	193
Kivel szemben szabható ki bírság?	194
A bírsággal sújtható személyi kör meghatározása – az előrelépés lehetősége a védelmi lépcsőn	195
Közhatalmi szervek bírságolása	196

Az előrelépés lehetősége a védelmi lépcsőn	198
Egységes bírságolási gyakorlat az unió tagállamaiban a védelmi lépcső fényében	199
Együttműködési eljárások és vitarendezés, hatóságok függetlensége	201
A jelenlegi szabályozás jellemzői – az együttműködés főbb szabályai – egyablakos ügyintézés és vitarendezés	201
A felügyeleti hatóságok függetlenségéről	204
A függetlenség kritériumai	206
A közös hatáskörgyakorlás intézményi reformja – az előrelépés lehetősége	214
Végkövetkeztetések	217
A védett jog tartalma	217
A védelmi lépcső elmélete	217
A védelem komponensei és minőségi mutatói	218
Az adatvédelmi tisztviselő szerepének megújításáról a védelmi lépcső fényében	218
Az adatvédelmi felügyeleti hatóság feladatellátásának új modellje a védelmi lépcső alkalmazásával	220
A felügyeleti hatóságok hatáskörének elemzése a védelmi lépcső alapján	221
Az adatvédelmi bírság elemzése a védelmi lépcső elmélete alapján	222
Az adatvédelmi hatóságok szerepéről	224
A látencia tagadása – nagyobb adatkezelői transzparencia	225
Állami példamutatás	226
A Rendelet kétéves alkalmazásának értékelése	227
Zárszó	228
Felhasznált irodalom	229
Szakirodalom	229
Intézményi dokumentumok	233
Egyéb forrás	235
A 29. cikk szerinti adatvédelmi munkacsoport munkássága – időrendi sorrendben	235
Az Európai Bizottság dokumentumai – időrendi sorrendben	236
Internetes források	237
Hivatkozott magyar bírósági ítéletek	237
Hivatkozott egyéb ítéletek	237
A Nemzeti Adatvédelmi és Információszabadság Hatóság ügyei	238
Az Emberi Jogok Európai Bíróságának hivatkozott ítéletei	238
Az Európai Unió Bíróságának hivatkozott ítéletei	239
Hivatkozott jogszabályok, egyezmények	240

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 jogász 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 jogász pályán. Az értekezésben körüljárt kérdések, a különböző védelmi szintek összehasonlítására tett javaslat, a védelmi lépcső gondolata mind ebből a jogász alaplásból 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 határfokú 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 élik 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. Végző soron ezért dolgozunk, ezért van értelme a mindennapi munkánknak, és így lehetünk majd talán elégedettek, amikor évtizedek múltán visszatekintve azt mondhatjuk: mi is hozzá tettünk 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 *privacy*-t 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.<sup>1</sup>

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.<sup>2</sup>

Jóri András szerint „az adatvédelmi jog célja a magánszféra védelme”.<sup>3</sup> A magánszféra, valamint a személyes adatok védelme az Alaptörvényben

<sup>1</sup> 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.

<sup>2</sup> Majtényi László így fogalmaz: „Az adatvédelem a személy, az ember, más szóval: az adatlany 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.

<sup>3</sup> Jóri András: *Adatvédelmi kézikönyv*. Budapest, Osiris Kiadó, 2005. 11.

rögzített,<sup>4</sup> 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<sup>5</sup> még nem hivatkozhatott az Európai Unió Alapjogi chartájára,<sup>6</sup> mindazonáltal a jogalkotás mögött ott húzódtott a tagállamok alapjogi hagyománya<sup>7</sup> 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 eljárássai 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.

<sup>4</sup> A magán- és családi élet, valamint a személyes adatok védelméhez fűződő jogot az Alaptörvény VI. cikke rögzíti.

<sup>5</sup> 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.

<sup>6</sup> 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.

<sup>7</sup> 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 preambulumbekzdésekben 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 védeljás 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) koncentrálok. 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.<sup>8</sup> 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 életeteket, élethelyzeteket, emberi kapcsolatokat képes befolyásolni. Az Európai Unió válasza ebben a tekintetben egyértelmű: „ami jogellenes offline, annak online is jogellenesnek kell lennie”.<sup>9</sup>

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 bízta a jogi megfelelés helyes módjának megtalálását. A korábbi szabályozáshoz képest

<sup>8</sup> 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.

<sup>9</sup> 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.<sup>10</sup> A szabályozásnak természetesen velejárója marad a kikényszerítés eszköztársa, de ez is összetettebbé válik a korábbiakhoz képest. Egységes gazdasági térben kívánja az uniós jogalkotó a védelmi szintet fenntartani, illetve megerősíteni; a megerősített hatóságokat uniószerre 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.<sup>11</sup> A közösségi oldalak piacáról kiderült, hogy már messze nemcsak közösségi oldalak, hanem jóval többet jelentenek annál. Az életviszonyokat befolyásolni képes gépezetté nőttek ki magukat. Erről írnak részletesen Brendan van Alsenoy és szerzőtársai.<sup>12</sup> A nyitott társadalmú demokráciák azzal szembesülnek, hogy választóik magatartása a róluk kialakított profilok alapján befolyásolhatóvá válik, a választási csatlások új dimenzióját nyitva meg.<sup>13</sup> Mindeközben a felhasználók a különböző nemzetbiztonsági szolgálatok hozzáféréseivel kapcsolatos hírek, így az Edward Snowden nevéhez fűződő kiszivárogtatások<sup>14</sup> 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-

<sup>10</sup> 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.

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

<sup>12</sup> 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.

<sup>13</sup> 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.

<sup>14</sup> 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.<sup>15</sup> Bár a big data kapcsán nehéz egységes definíciót találni, Zódi Zsolt szemléletesen fogalmazza meg: a jelenség lényege, hogy a külvilág és az emberek egyre több adatát rögzítik, és ezekre az adathalmazokra egyre többféle elemző, profilírózó, következtető és jósló algoritmus épül.<sup>16</sup> 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.<sup>17</sup> Orla Lynskey az adatok koncentrációját és a kapcsolódó hatalmi helyzetet elemezve mutat rá az „adathatalom” jelenségére, amelynek privacyszempontból is különös figyelmet kell szentelni.<sup>18</sup>

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 érdekvédelem érdekében három lehetséges utat javasol: erősebb adatvédelmi kikényszerítést, vagy az adatok közjósággént, 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-

<sup>15</sup> 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.

<sup>16</sup> Vö. Zódi Zsolt: Privacy és a Big Data. *Fundamentum*, 21. (2017), 1–2. 18.

<sup>17</sup> 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.

<sup>18</sup> Vö. Orla Lynskey: Grappling with “Data Power”: Normative Nudges from Data Protection and Privacy. *Theoretical Inquiries in Law*, 20. (2019), 1. 189–220.

egyvezetethetetlenek.<sup>19</sup> Négy példát is említ erre: a célhoz kötöttség 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.<sup>20</sup>

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.<sup>21</sup>

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,

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

<sup>20</sup> 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.

<sup>21</sup> 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.<sup>22</sup> Nicholas Diakopoulos szintén az átláthatóság mellett érvel, és az egyébként a magánszféra védelmére is használható algoritmusok kapcsán a rajtuk keresztül használt hatalom tisztázását szorgalmazza.<sup>23</sup> Eszteri Dániel a mesterséges intelligencia és a GDPR elemzése kapcsán kiemeli az emberi beavatkozás szükségességét, a tisztességes adatkezelés követelményeit.<sup>24</sup> 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”.<sup>25</sup> 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.<sup>26</sup> Az informatikai megoldások a folyamatosan bővülő igényekhez dinamikusan alkalmazkodnak, amelyek újabb és újabb kérdéseket vetnek fel a technológia és az adatvédelem határán.<sup>27</sup>

<sup>22</sup> 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.

<sup>23</sup> Nicholas Diakopoulos: *Algorithmic Accountability Reporting: on the Investigation of Black Boxes*. Columbia Journalism School – Tow Center for Digital Journalism, 2013.

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

<sup>25</sup> Eszteri (2019): i. m. 671.

<sup>26</sup> A felhőszolgáltatásokra vonatkozó jogi szabályozás szükségességéről vö. Váradai 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.

<sup>27</sup> A legújabb ködrendszerekre vonatkozó adatvédelmi szabályokról lásd bővebben: Gizem Gültekin Várkonyi – Váradai 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.