SZEGEDI LÁSZLÓ – DORNFELD LÁSZLÓ – POLGÁR ZOLTÁN – TELEKI BÁLINT*

A GDPR ALKALMAZÁSÁVAL KAPCSOLATOS ELSŐ TAGÁLLAMI TAPASZTALATOK – EGYSÉGES SZABÁLYOZÁS, ELTÉRŐ ALKALMAZÁS?

Két éve lépett hatályba az új uniós adatvédelmi rezsim, a GDPR. A szabályozás alapkoncepciója az egységesség volt, a bírságolás kapcsán azonban a tagállami gyakorlat egészen mást mutat. Ez különösen a technológiai óriásvállalatok körében jelent problémát, amelyek megpróbálhatnak a forum shopping eszközeivel élni a bírságok elkerülésére vagy mérséklésére. A tanulmányban elemzésre kerül a szabályozás, valamint az ír és magyar bírságolási gyakorlat

1. A GDPR szerepe és szabályozási koncepciója

1.1. Az uniós adatvédelem belső piaci keretei

Az európai integráció egyik egyértelmű problémája az uniós rendelkezések végrehajtásáért felelős tagállami szinten (közvetett végrehajtás) a végrehajtási deficit jelensége. Az egyes szakpolitikai területeken az uniós és a tagállami hatáskörök megosztottsága miatt eltérő a szabályozás kidolgozottsága, így a végrehajtási deficitet is érdemes ágazati jelleggel megvizsgálni.[1] A tagállamok máig (relatív) *autonómiával* rendelkeznek a közigazgatási szervezetrendszerük kialakítását, az eljárási követelményeket (ebbe beleértve a közigazgatási szankciórendszerük kialakítását) illetően is.[2] Az uniós jogalkotó – a végrehajtási deficit leküzdése érdekében – egyre több esetben az uniós jog végrehajtásáért közvetlenül felelős uniós szerveket és intézményeket hoz létre, vagy ilyen hatásköröket biztosít már meglévő uniós szerveknek, intézményeknek (közvetlen végrehajtás erősödése). Sok esetben viszont megmarad a tagállami szervek elsődleges fellépési lehetősége az uniós jog végrehajtása során, de a belső piac keretei között eltérő mechanizmusok alakultak ki az egységes jogalkalmazás biztosítása érdekében.[3] Ennek további feltétele az egységes uniós szabályozás irányába tett elmozdulás, amelynek egyik legújabb példája a korábbi irányelvet felváltó új uniós adatvédelmi rendelet (GDPR)[4] elfogadása.

Az ágazati szabályozás szempontjából az adatvédelmi terület kiemelt fontosságúvá vált az utóbbi évtizedekben. Ez nem pusztán az uniós hatáskörök bővülésével és a belső piac folyamatos fejlődésével függ össze, hanem egyértelmű velejárója a 2000-es évek infokommunikációs forradalmának is. A mindennapi életünket alapvető módon átalakító technológiai változás nem pusztán pozitív hozadékokkal járt, hiszen a személyes adatok védelme, a bioetikai dilemmák megsokszorozódása, a robotika térhódítása egyértelmű szabályozói, valamint hatékony végrehajtási válaszokat követel meg. Utóbbi viszont nehezen képzelhető el a nemzetállami keretek között, már csak annak okán is, hogy a technológiai és infokommunikációs iparág szereplői méretüket, jelentőségüket tekintve globális szintű tényezőkké váltak, amelyek működésének egységes (belső) piaci szabályozása és felügyelete nem pusztán az uniós polgárok érdekei, hanem az Unió mint gazdasági egység szempontjából is elengedhetetlen.

Célunk jelen írással a GDPR alkalmazásának kapcsán felmerült egyes tagállami gyakorlatok bemutatása, illetve azok összevetése a GDPR bizonyos rendelkezéseivel, valamint az ahhoz kapcsolódó tágabb értelemben vett uniós adatvédelmi követelményekkel. Tekintettel az ezen uniós rendelet hatálybalépése óta eltelt viszonylag rövid időre, átfogó jellegű elemzés felvázolására nincs mód. Ugyanakkor már látható, hogy az egyes adatvédelmi rendelkezések alkalmazása kapcsán milyen dilemmák vetődnek fel. Röviden ezen jelenségekre kívánunk reflektálni az említett technológiai nagyvállalatok szempontjából, a GDPR szerinti illetékesség miatt releváns ír példa, valamint a hazánkban megjelenő egyes gyakorlati kérdések elemzésével. Az igencsak eltérő jogrendszerek kapcsán felvetődik a kérdés, hogy a hasonló adatvédelmi dilemmákra adott válaszaik jelzik-e már az egységes (egységesülő) gyakorlat irányába való haladást, hogy melyek az együttműködés keretei, milyenek a piaci szereplők esetleges válaszai a GDPR azonos védelmet garantálni kívánó szabályozására és annak tagállami alkalmazására.

1.2. Az egységes adatvédelmi gyakorlat kialakításának szervezeti rendje

A 95/46/EK irányelvet[5] felváltó GDPR-t elsődlegesen változatlanul a tagállami hatóságok alkalmazzák. Így a közvetett végrehajtás meghatározó szerepe adatvédelmi területen is megmaradt. Ugyanakkor a korábbi joggyakorlat egyértelműen rámutatott, hogy új alapokra kell helyezni az egyes tagállami hatóságok közötti együttműködés, vitarendezés és egységes gyakorlat kialakításának kereteit. Utóbbi kérdések rendezése szempontjából kiemelkedő fontosságú új szereplő az uniós ügynökségként létrehozott Európai Adatvédelmi Testület (*European Data Protection Board*, a továbbiakban: EAT). Ennek elődje az 29. cikk szerinti munkacsoport (a továbbiakban: munkacsoport), amelynek szervezeti kereteit (titkárságát) az Európai Bizottság biztosította.[6] Mind a munkacsoport, mind az EAT meghatározó szerepet kapott és kap a kapcsolódó szabályozás egységes értelmezésének lefektetésében.

Az Európai Unió Bíróságának (a továbbiakban: EUB) korábbi joggyakorlata alapján is felmerült problémaként az, ha az adatvédelmi eljárás lefolytatása több tagállamot is érintett. A tagállami felügyeleti hatóság érintettsége fennállhat a GDPR 4. cikk 22. pontja szerint a tevékenységi hely; a lakóhellyel rendelkezők jelentős mértékben érintettsége; valamint a panaszbenyújtás helye alapján.[7] A GDPR 4. cikk 23. pontja pedig külön kategóriaként kezeli a „személyes adatok határokon átnyúló adatkezelését", amely „több tagállamban tevékenységi hellyel rendelkező adatkezelő vagy adatfeldolgozó több tagállamban található tevékenységi helyein folytatott tevékenység" vagy több tagállamban jelentős mértékben vett érintettség alapján áll fenn. Emellett a munkacsoport is külön iránymutatást bocsátott ki, hogy a tagállami hatóságok közül egyértelműen ki lehessen jelölni a fő felügyeleti hatóságot.[8]

A GDPR külön fejezetben foglalkozik az együttműködési és az egységességi eljárások részletes szabályaival. Az *együttműködési eljárásban* a tagállami hatóságok fő felügyeleti hatóságként, vagy érintett felügyeleti hatóságként járhatnak el. A fő felügyeleti hatóságként eljáró tagállami hatóság feladata, hogy a döntéshozatali folyamatban együttműködjön az érintett felügyeleti hatóságként eljáró tagállami hatóságokkal és koordinálja az eljárást, emellett a részt vevő hatóságok kölcsönösen segítséget nyújtanak egymásnak, valamint közösen hajthatnak végre műveleteket.[9] Az *egységességi mechanizmus* pedig az egységes jogalkalmazást biztosító eljárások összességét jelenti. A mechanizmus esetében a főszerep már az EAT-nak jut. Az EAT-ot a tagállami hatóságnak tájékoztatnia kell elsődlegesen szabályozási jellegű döntéstervezeteiről, amely nem fogadható el, mielőtt azt az EAT nem véleményezi.[10] Ha az előbbi esetben

* Szegedi László: egyetemi adjunktus, Nemzeti Közszolgálati Egyetem, Államtudományi és Nemzetközi Tanulmányok Kar, Európai Köz- és Magánjogi Tanszék
Dornfeld László: A Mádl Ferenc Összehasonlító Jogi Intézet kutatója, doktorjelölt
Polgár Zoltán: A Nemzeti Közszolgálati Egyetem Közigazgatás-tudományi Doktori Iskola doktorandusza
Teleki Bálint: A Nemzeti Közszolgálati Egyetem Közigazgatás-tudományi Doktori Iskola doktorandusza

nem jut konszenzusra az EAT és a tagállami szint, vagy ha a tagállami hatóságok együttműködésében nincs konszenzus, vagy a tagállami hatóságok között illetékességi vita merül fel, az EAT vitarendezési eljárásában kötelező erejű döntést fogad el – amely a tagállami hatóságok között fennálló vita esetén kizárja a végleges döntés elfogadását.[11] Az EAT az egységességi mechanizmus és jogértelmezés érdekében véleményt ad ki.[12]

Az egységes adatvédelmi gyakorlat kialakításához szorosan hozzátartozik az adatvédelem harmadik országbeli hiányosságainak ellensúlyozása. Az ellensúlyozás eszközeit már a GDPR Preambulumának (108) pontja felsorolja. Az eszközök az alábbiak: a kötelező erejű vállalati szabályok, a Bizottság által elfogadott általános adatvédelmi kikötések, a felügyeleti hatóság által elfogadott általános adatvédelmi kikötések vagy a felügyeleti hatóság által engedélyezett általános szerződési feltételek alkalmazása.

A kötelező erejű vállalati szabályok (BCR) lényegében a személyes adatok védelmére vonatkozó szabályzat, amely biztosítja, hogy az Európai Unió adatvédelme az adattal együtt „utazzon" a vállalat szervezetén belül. Ha valamely vállalat BCR-t kíván megalkotni, akkor figyelembe kell vennie a GDPR 47. cikkében előírt kötelező tartalmi elemeket, valamint az EAT által kiadott iránymutatásokat, munkadokumentumokat. Az egységesség érdekében az EAT elfogadta a WP 263 rev. 01 számú munkadokumentumot. [13]

1.3. Az egységes szankcionálási gyakorlat kialakításának keretei

Jogsértések esetén az illetékes (tagállami) felügyeleti hatóság a GDPR 58. cikk (2) bekezdése által felkínált korrekciós intézkedéseket alkalmazza. A GDPR által felkínált intézkedések rendszere eleve az egységes (egységesülő) jogalkalmazás irányába hat, bár a hatóságok többféle intézkedést szabhatnak ki akár együttesen, akár külön-külön is. Emellett a munkacsoport *soft law* jellegű iránymutatást fogadott el a közigazgatási bírságok alkalmazásáról és megállapításáról.[14] Túl az egyes tagállami jogrendszerek jellegzetességein (hatóságok helyett bíróságok szabhatnak ki bírságot),[15] a tagállamok közigazgatási szankciórendszerére kiható tágabb értelemben európai,[16] szűkebb értelemben vett uniós jogi tendenciák[17] egyértelműen megmutatkoznak, amelyet ágazati szinten a GDPR és az iránymutatás tovább erősít.

A GDPR célja a szankciók szigorítása és harmonizálása, melynek érdekében minden tagállam felügyeleti hatósága bírságolási hatáskörrel rendelkezik.[18] A GDPR rögzíti annak követelményét is, hogy azonos szintű védelmet kell biztosítani, és az egyes jogsértőkre azonos szankciókat kell alkalmazni.[19] Emellett el kell kerülni, hogy a hatóságok hasonló ügyekben különböző korrekciós intézkedéseket alkalmazzanak.[20] Túl a tagállamon belüli egységes gyakorlaton, ez a dilemma értelemszerűen lényeges lesz a tagállamok közötti relációban. A kapcsolódó iránymutatás azt is lefekteti, hogy a tagállami hatóságok együttműködési mechanizmusok révén együttműködnek egymással és – adott esetben – az Európai Bizottsággal, például munkaértekezletek rendszeres tartása útján, amely az iránymutatás újbóli megvizsgálásához (felülvizsgálatához) is vezethet.[21]

A GDPR 83. cikk (2) bekezdése több mérlegelendő szempontot határoz meg a tagállami hatóságok számára, amelyeket figyelembe kell venniük annak eldöntésekor, hogy szükség van-e a közigazgatási bírság kiszabására, illetve az összeg megállapításakor – amely eleve feltételezi az egyedi értékelés követelményét.[22] A bírság kiszabásakor és mértékének meghatározásakor figyelembe kell venni az alábbi tényezőket: a jogsértés természete, felróhatóság, kár enyhítése érdekében tett intézkedések, adatkezelő vagy adatfeldolgozó felelősségének a mértéke, korábbi releváns jogsértések, a felügyeleti hatósággal folytatott együttműködés, a jogsértéssel érintett személyes adatok kategóriái, a felügyeleti hatóság tudomásszerzése a jogsértésről, a korrekciós intézkedések végrehajtása, a magatartási kódex alkalmazása, egyéb súlyosító/enyhítő körülmények.[23]

A bírság mértéke (összege) tekintetében a GDPR felső határokat fektet le (10, ill. 20 millió euró, vagy a vállalkozás éves világpiaci forgalmának adott 2, ill. 4%-a) amely előrevetíti, hogy a GDPR egyes rendelkezéseinek megsértése más rendelkezések megsértéséhez képest súlyosabbnak minősülhet. Az illetékes felügyeleti hatóság ugyanakkor az eset körülményeinek a 83. cikk (2) bekezdésében foglalt általános szempontok fényében történő értékelése során dönthet úgy, hogy jobban vagy kevésbé szükséges, hogy közigazgatási bírság formájában kerüljön sor korrekciós intézkedésre.[24] Emellett pedig a bírság alóli mentesülés kereteit is lefekteti a GDPR egyes speciális címzetti kategóriáknál, így a közhatalmi, vagy egyéb közfeladatot ellátó szervekkel, vagy adatkezelő természetes személyekkel szemben.[25]

2. A GDPR-ral kapcsolatban kialakuló tagállami gyakorlatok

2.1. A GDPR és az ír adatvédelmi gyakorlat

A GDPR-t megelőzően Írországban az 1988-as, 2003-ban módosított adatvédelmi törvény (a továbbiakban: *Data Protection Acts 1988–2003*) jelentette az adatvédelmi szabályozás legfontosabb normáját. Ezen törvény felhatalmazó rendelkezései alapján az adatvédelmi hatóság megalkotott egy *Code of Practice* elnevezésű *soft law* dokumentumot az adatvédelmi incidensekkel kapcsolatos eljárásokra.[26] A GDPR követelményeinek való megfelelés érdekében az ír jogalkotó új adatvédelemi törvény megalkotása mellett döntött. Így a *Data Protection Acts 1988–2003*-at felváltotta a *Data Protection Bill 2018*, amely 2018. május 24-én lépett hatályba.

Létrejött adatvédelmi hatóságként az Adatvédelmi Bizottság (mint GDPR-konform tagállami hatóság, azaz DPA, a továbbiakban: *Irish Data Protection Commission,* IDPC), amelynek legfeljebb három tagja lehet, akiket a kormány jelöl ki erre a feladatra. A legmagasabb adatvédelmi hivatalt 2014 óta különböző címeken betöltő Helen Dixon jelenleg az egyetlen *commissioner*.[27] Megjegyzendő egyébként, hogy a jogelőd adatvédelmi hatóságot is ugyanígy hívták az előző törvény szóhasználata szerint.[28]

További fontos pont az új adatvédelmi törvényben a tagállami székhelyű közhatalmi, vagy egyéb, közfeladatot ellátó szervvel szemben kiszabható bírság szabályozása. A GDPR 83. cikk (7) bekezdése alapján a tagállamok maguk dönthetik el, hogy a fenti szervtípusokkal szemben kiszabható-e – természetesen a GDPR tárgyi hatályán belüli ügyek tekintetében – közigazgatási bírság, és ha igen, milyen mértékű. Az ír törvényhozás hosszas vita után 1 millió eurós limitben határozta meg a fenti szervtípusokkal szemben kiszabható bírság mértékét, elsősorban azon megfontolás mentén, hogy az ennél nagyobb összegű bírságok adott esetben az érintett szerv működését veszélyeztethetnék.[29]

Írország számos Európán kívüli, elsősorban a kaliforniai Szilícium-völgyből származó technológiai óriásvállalat – az IT-szektorban globálisan piacvezető vállalat – európai központja, ezek közül is kiemelkedik a Google és a Facebook. Az adatvédelmi rezsimből fakadó előnyökön túl Írország adókedvezményeket és egyéb ösztönzőket is bevetett annak érdekében, hogy az USA és Kanada multinacionális vállalatai Írországot válasszák európai központjuknak.[30] A Deloitte vonatkozó országismertetője alapján Írország 2017-ben a világ második legnagyobb szoftverexportőre volt, köszönhetően az ott letelepedett technológiai vállalatok nagy számának. A társadalombiztosítási hozzájárulás az egyik legalacsonyabb a világon, a társasági adó lehet akár 0% is a megfelelő feltételek teljesülése esetén, a részvénykibocsátás illetéke pedig mindig 0%, és ezek csak a leglátványosabb ilyen természetű előnyök.[31]

A GDPR-szabályozás értelmében a fentiekben ismertetett illetékességi rendszer keretei között, a fenti vállalatok esetében *fő hatóságként* az ír adatvédelmi hatóság jár el.[32] Írországot több alkalommal érte kritika, hogy nem lép fel kellő eréllyel a technológiai óriásvállalatok adatvédelmi természetű visszaéléseivel, jogsértéseivel szemben, és ez a tendencia már a GDPR hatálybalépése előtti időkben megjelent. Kritizálták Írországot 2011-ben, amikor a Facebook külső alkalmazásoknak adott át a felhasználók ismerőseivel kapcsolatos adatokat, hasonlóan 2014-ben, amikor a Facebook az általa

újonnan megvásárolt WhatsAppnak adott át személyes adatokat, ugyanis Írország egyik esetben sem lépett fel hatékonyan Facebookkal szemben. A Google egyes termékei (YouTube, Gmail, Google Photos, stb.) közötti gyanús adatáramlás tekintetében is igencsak elhúzódott a vizsgálat megkezdése 2018-ban. Már a GDPR bevezetése utáni első 10 hónapban számos ország adatvédelmi szakértői, adatvédelmi kutatói, akadémikusai fejezték ki fokozott aggodalmukat azzal kapcsolatban, hogy a GDPR sérülékeny lehet a technológiai óriásvállalatok tekintetében egy rendelkezés miatt, nevezetesen, hogy a fő hatóság abban az országban legyen, ahol ezen cégek adatkezelői találhatók – és ez a legtöbb esetben Írország.[33]

A helyzet megértését segítik az ún. Schrems-ügyek is, amelyeket Maximillian Schrems osztrák ügyvéd indított, és amelyekben az EUB előzetes döntéshozatali eljárás keretében foglalt állást. A 2014. évi Schrems I. ítélettel[34] sikerült elérni, hogy az addig az USA-beli vállalatok önminősítésén alapuló, az USA Kereskedelmi Minisztériuma *(U.S. Department of Commerce)* által kiadott „*safe harbor*" követelményeknek megfelelő és az Európai Bizottság határozata által is akként elismert vállalatokat is megvizsgálhassák az EU tagállami adatvédelmi hatóságai. Erre akkor kerülhet sor, amennyiben a harmadik ország felé történő adattovábbítás kapcsán felmerül, hogy a harmadik ország jogrendszere nem biztosítja a megfelelő védelmi szintet az erre hivatkozó személy személyes adatokkal kapcsolatos jogai és szabadságai tekintetében. Ennek következtében került sor az EU és az USA közötti tárgyalásokra, amelyek a *Privacy Shield* elnevezésű megegyezéssel rendezték a helyzetet.[35] Utóbbi alapvetően egy olyan keretegyezmény, amelyet az USA Kereskedelmi Minisztériuma, valamint az Európai Bizottság és Svájc dolgozott ki annak érdekében, hogy az érintett felek vállalatai az Atlanti-óceán mindkét felén rendelkezzenek egy olyan mechanizmussal, amely lehetővé teszi a személyes adatok továbbítását az EU-ból és Svájcból az USA-ba.[36] A Schrems II. ügyben[37] 2020. július 16-án hozott ítéletében az EUB ezen megállapodást semmisítette meg, amely nyomán a nemzetközi adattovábbítás egy új rendszerét lesz szükséges kidolgozni az EU és az USA között. A *Privacy Shield* rendszerében a https://www.privacyshield.gov oldalon listázott amerikai cégeket a megállapodás értelmében az európai uniós adatvédelmi követelményeknek megfelelőnek kellett tekinteni, ugyanakkor meglehetősen átláthatatlan volt, hogy adott vállalat vagy szervezet hogyan kerülhet fel a listára.[38]

A számmal jelölt Schrems-ügyek mellett létezik egy a Schrems által indított harmadik ügy is, amely jelentőséggel bír, ez a *Schrems v. Facebook Ireland Limited ügy*,[39] ennek jelentősége inkább a fogyasztóvédelem kollektív jogorvoslati dimenziója tekintetében érvényesül, ugyanakkor szintén rámutat bizonyos hiányosságokra.[40] Schrems 2019-ben, amikor az ír adatvédelmi gyakorlat fejlődéséről kérdezték, szó szerint azt nyilatkozta, hogy: *„They've basically gotten smarter about not doing things"* („Egyre ügyesebben tesznek semmit"). Ezalatt azt értette, hogy az ír hatóság vállalatbarát módon áll a technológiai óriásvállalatokkal szembeni (adatvédelmi) panaszokhoz.[41] Schrems már 2013-ban azért kényszerült az osztrák hatóságok előtt indítani eljárást, mert az ír hatóságok rendkívül lassan jártak el az ügyben.[42]

2.2. Az ír adatvédelmi szankcionálási és bírságolási gyakorlat

Az IDPC saját statisztikái alapján a 2018. május 25. és 2020. május 25. közötti időszak, vagyis a GDPR hatályábalépése óta eltelt két év alatt 15 025 aktát nyitott egyének jogsérelme miatt, ezek 80%-át sikerült is lezárniuk, és 12 437 adatvédelmi incidenssel kapcsolatos ügy indult, amelyek 94,88%-át sikerült lezárniuk. Felügyeleti hatáskörben eljárva 53 tagállami szintű és 24 határon átívelő nyomozást bonyolítottak le hivatalból, illetve más tagállamok adatvédelmi hatóságainak kezdeményezésére.[43]

Az IDPC honlapján elérhető tájékoztatás alapján 2019-ben, valamint 2018-nak a GDPR hatálybalépését követő időszakában a GDPR hatálya alá tartozó ügyben nem született bírsággal végződő döntés. A 2020-ban kiszabott bírságok összértéke 715 000 euró, az egy bírsággal záruló ügyre vetítve átlagosan 143 000 euró. Ez a szám azonban torzít, hiszen a közhatalmat gyakorló, illetve egyéb közfeladatot ellátó szervek esetében az ír szabályozás és gyakorlat jelentősen mérsékeli a bírságot.

Az IDPC tájékoztatója[44] alapján eddig összesen 4 ügy zárult bírsággal (valójában 5, de a legutóbbi ügy még nincs feltüntetve a weboldalon), ebből 3 ugyanazon ügyféllel szemben. A *Tusla Child and Family Agency*t 2020. április 7-én kelt határozatban 75 000 euró összegre, 2020. május 21-én kelt határozatban 40 000 euró összegre bírságolták meg, a nem megfelelő szintű biztonsági intézkedések, valamint az adatvédelmi incidens késedelmes bejelentése miatt.[45] 2020. augusztus 12-én kelt határozatban egy 50 000 és egy 35 000 eurós bírságot is kaptak, az előbbiekben említett problémák mellett itt még jogsértőnek ítélte a hatóság, hogy nem volt biztosított, hogy az adatfeldolgozó csak az adatkezelő utasításai mentén járjon el, valamint a GDPR alapelvei közül a „pontosság" elvét is megsértették.[46] A bírságon túl egyéb intézkedések is alkalmazásra kerültek a jogsértő helyzet megszüntetése végett, így a hatóság elmarasztalta az ügyfelet *(„reprimand")*, és kötelezte olyan szervezeti változások megtételére, amelyek a jogszerű állapot eléréséhez szükségesek.

A *Health Service Executive*-ot 2020. augusztus 18-án kelt határozatban 65 000 euró összegre bírságolták meg nem elégséges szintű – technikai és szervezeti értelemben vett – biztonsági intézkedések miatt, valamint a GDPR alapelvei közül az „integritás és bizalmas jelleg" elvének megsértése miatt. A *Cork University Maternity Hospital*-ban az előbbiek szerint nem megfelelően kezelték a páciensek adatait, különösen papíralapú dokumentumok esetében.[47] A bírságon túl a hatóság elmarasztalta az ügyfelet, és kötelezte a dokumentációs gyakorlatuk jogszerű irányba való átalakítására.

További három ügy *(An Garda Síochana, Kerry County Council és Waterford City and County Council)* bírság kiszabása nélkül, egyéb intézkedések alkalmazásával zárult. Ezeket az ügyeket az köti össze, hogy mindegyik esetben a zártláncú kamerás megfigyelőrendszer (CCTV) alkalmazásának – drónok rendészeti célú használatát is beleértve – módja, valamint a kapcsolódó belső szabályzatok hiánya vagy nem megfelelő volta miatt volt az adatkezelés jogsértő. A hatóság ezekben az esetekben – részben az ügyfelek együttműködése miatt – megelégedett a marasztalással, a problémás rendszerek átmeneti letiltásával, és a jogszerű gyakorlat kialakítására való kötelezéssel.

A fentebb már említett, a GDPR hatálybalépését követő első két évét elemző jelentés szerint, számos vizsgálat indult 2018 májusa óta a technológiai óriásvállalatok ellen, ezek kimenetele azonban még nem ismert, de van olyan, ahol már visszavonták a panaszt. Multinacionális technológiai vállalatok ellen összesen 24 vizsgálat indult a GDPR alapján, ezek megoszlása: a Facebook-csoport ellen 11 (amelyből a Facebook ellen 8, a WhatsApp ellen 2 és az Instagram ellen 1); az Apple ellen 3; a Twitter ellen 3; a Google ellen 2; a LinkedIn, a Tindert üzemeltető MTCH Technology Services, a Quantcast, a Verizon és a Yelp mindegyike ellen 1–1).[48] Ezek az ügyek tehát láthatóan elhúzódnak valamelyest, de rendkívül tanulságos lesz megfigyelni, hogy milyen eredménnyel zárulnak majd le.

A fentiek alól egy kivétel látunk, a *Twitter International Company* esetében egy 450 000 eurós közigazgatási bírság került kiszabásra 2020. december 9-i hatállyal. A jogsértést egy adatvédelmi incidens késedelmes bejelentése, illetve a bejelentéshez kapcsolódó dokumentációs kötelezettségek nem elégséges teljesítése jelentette.[49] Az IDPC a rendelkezésre álló adatok alapján a vállalat éves forgalmát 3,46 milliárd USD-ben állapította meg. Ez alapján, a GDPR 83. cikk (4) bekezdésében foglaltakra támaszkodva, a 2%-os kulcs alkalmazása mellett a maximálisan kiszabható bírságot 69,2 millió USD-ben határozta meg. Az IDPC figyelembe vette, hogy a vállalat együttműködött, és hogy a bírságnak hatékonynak kell lennie, de nem szabad meghaladnia a szükséges mértéket, így a bírságot 500 000 USD, azaz átváltva kerekítéssel 450 000 euró összegben állapította meg. A bírság mellett a hatóság elmarasztalta az ügyfelet. Az adatszivárgást jelentő informatikai problémát az ügyfél nem sokkal annak jelentkezése után önként elhárította.[50]

Több az EUB előtt folyamatban lévő ügy is utalhat arra, hogy a viszonylag megengedőnek tűnő ír gyakorlat léte az érintett technológiai vállalatok számára is nyilvánvaló. Felhasználók beleegyezése nélküli adatvédelmi jogsértés miatt a Facebook Belgium leányvállalat a kapcsolódó ügyben arra hivatkozott, hogy a GDPR hatálybalépése után a belga adatvédelmi hatóság nem jogosult az eljárás folytatására, mivel kizárólag a Facebook Unión belüli tevékenységi központja szerinti állam adatvédelmi hatósága (vagyis az IDPC) jogosult bírósági eljárást indítani a határokon átnyúló adatkezelés megsértése miatt. Az időközben megszületett ítélet szerint adott feltételek teljesülése esetén a fő felügyeleti hatóságtól eltérő tagállami felügyeleti hatóság is e tagállam bírósága előtt keresetet indíthat, mind az adatkezelőnek az említett hatóság tagállamában található tevékenységi központja, mind pedig ezen adatkezelő más tevékenységi helye tekintetében.[51] Az ítélet pedig kiemeli a határon átnyúló adatkezelések tekintetében a fő és a többi érintett hatóság közötti együttműködés fontosságát, ennek keretein belül a fő felügyeleti hatóság nem hagyhatja figyelmen kívül a többi érintett felügyeleti hatóság álláspontját, utóbbi hatóságok által emelt bármely releváns és megalapozott kifogás ideiglenesen megakadályozza a fő felügyeleti hatóság döntéstervezetének elfogadását.[52] Itt szükséges megjegyezni, hogy az Európai Parlament 2021. május 20-án határozatot fogadott el, amelyben a képviselők felszólítják az Európai Bizottságot kötelezettségszegési eljárás lefolytatására Írországgal szemben, mivel álláspontjuk szerint az ország nem hajtja végre megfelelően a GDPR rendelkezéseit, kifejezetten az elhúzódó adatvédelmi hatósági eljárásokat tartják aggályosnak, és különösen a technológiai óriásvállalatokkal kapcsolatos ügyekben.[53] A francia adatvédelmi hatóság (*Commission Nationale de l'informatique et des Libertés* – CNIL) 50 millió eurós bírságot szabott ki a Google LL.C.-re. Utóbbi is megpróbált arra hivatkozni, hogy a francia hatóság helyett az IDPC-nek kellett volna eljárnia. Ezt az érvet a CNIL azzal utasította el – állást foglalva a tevékenységi központ kapcsán annak kérdésben –, hogy az adatkezelés céljára és eszközeire vonatkozó döntéseket nem az ír vállalatnál hozzák.[54]

Az ír gyakorlat az eddigiek alapján vegyesnek mondható, hiszen bár született nagyobb összegű bírság (kivétel a *Twitter International Company* esetében egy 450 000 eurós), ám az egyéb intézkedéseket is alkalmazzák. Emellett egyéb tagállami hatóságok kifejezetten nagy összegű bírságokat szabnak ki – több német ügyben is különös súllyal vették figyelembe a munkavállalók jogtalan megfigyelését.[55]

A hatékony hatósági fellépés számos egyéb tényezőtől is függhet. Ruohonen és Hjerppe nemcsak az ír, de majdnem az összes tagállami adatvédelmi hatóságokra vonatkozóan – de az ír példát elemezve részletesebben, demonstratív jelleggel – kimutatják, hogy az eredményes hatósági működést jelentősen befolyásolják az emberi erőforrás jellegű tényezők is. Ugyanis a legtöbb tagállamban nagyon kevés műszaki végzettségű technikai szakember dolgozik ezeknél a szerveknél, abszolút értelemben és az adott szerv összdolgozói létszámához viszonyítva is, amely az adatvédelmi területen megnehezíti a hatósági jogalkalmazást, mivel magának a problémának a megértése is gond lehet.[56] Ruohonen és Hjerppe utalnak továbbá a korábbi adatvédelmi irányelv idejéből származó tendenciákra, amelyeket a GDPR-rezsim is megörökölt. Ez részleteiben azt jelenti, hogy a transzparencia hiánya, az interkulturális konfliktusok, a DPA-k közötti megfelelő együttműködés hiánya – ugyanez igaz tagállami és uniós viszonylatban is –, a prioritások következetlen meghatározása és a gyakori, egyúttal túlzott tolerancia a jogsértésekkel szemben, valamint adott esetben a technikai felkészültség hiánya (személyi állomány és az infrastruktúra is), összességében jelentősen megnehezítik vagy ellehetetlenítik a hatékony hatósági fellépést. A szerzők hozzáteszik ugyanakkor, hogy ezeket a problémákat azért nem szabad túlértékelni, mert korántsem csak az adatvédelem területén vannak az uniós jog végrehajtásának ilyen természetű gondjai.[57]

2.3. A GDPR és a magyarországi adatvédelmi gyakorlat

Magyarországon is az ír példánál látott többlépcsős jogfejlődés zajlott le. 2012. január 1. és 2017. december 31 között, két jogszabály, a személyes adatok védelméről és a közérdekű adatok nyilvánosságáról szóló 1992. évi LXIII. törvény (Avtv.) és az információs önrendelkezési jogról és az információszabadságról szóló 2011. évi CXII. törvény (Infotv.) voltak az adatvédelmi terület fő jogszabályai. Emellett a közigazgatási hatósági eljárás és szolgáltatás általános szabályairól szóló 2004. évi CXL. törvény (Ket.), majd az általános közigazgatási rendtartásról szóló 2016. évi CL. törvény (Ákr.) határozta meg a hatósági jogalkalmazás általános kereteit. 2018. május 25-tel a szabályozási rendszer bővült a GDPR előírásaival. 2018. július 26-tal alakult ki a jelenleg alkalmazandó szabályozási rendszer, amikorra az Infotv. módosításai is hatályossá váltak.

Az Alaptörvény[58] elfogadása, valamint az Ombudsmantörvény[59] nagymértékben átalakították a személyes adatok védelmének és a közérdekű adatok nyilvánosságának magyarországi rendszerét, mivel elfogadásukkal egy új adatvédelmi felügyeleti rezsim kezdődött, és az ombudsmani rendszert hatósági rendszer váltotta fel. A 2012. január 1-jén megalakuló új hatóság (Nemzeti Adatvédelmi és Információszabadság Hatóság; a továbbiakban: NAIH), új apparátussal kezdte meg a működést. Az Infotv.-vel létrehozott Hatóság autonóm államigazgatási szerv, felettes szervvel nem rendelkezik, nem utasítható, szervezetileg és pénzügyileg önálló. Az Európai Unió adatvédelmi reformjával összefüggő módosításáról, valamint más kapcsolódó törvények módosításáról szóló 2018. évi XXXVIII. törvény, amely 2018. július 26-án lépett hatályba, módosította az Infotv.-t, és ez azt eredményezte, hogy a NAIH lett a GDPR-ban előírt tagállami felügyeleti hatóság (54. cikk).

Magyarország nem vált a technológiai óriásvállalatok székhely-, illetve tevékenységközpontjává, mint Írország. Ennek ellenére a magyarországi kötődésű adatvédelmi ügyek is hatással voltak a GDPR-ban megfogalmazott szabályozásra. A legismertebb ezek közül a *Weltimmo-ügy*,[60] amelyben még a korábbi irányelv értelmezése vált szükségessé. A Weltimmo-ügy annak a tipikus példája, amikor a szolgáltatás helye (annak hatása az uniós polgárokra és piaci szereplőkre) és a szolgáltató székhelye elválik egymástól. A gyakorlatban ez úgy valósult meg, hogy a Szlovákiában bejegyzett Weltimmo társaság egy magyarországi ingatlanokat hirdető weboldalt üzemeltetett. A hirdetések egy hónapig ingyenesek voltak, majd ezt követően a hirdetésért díjat kellett fizetni. Számos hirdető az ingyenes időszakot követő időszakra nézve elektronikus levélben kérte hirdetése és egyben a rá vonatkozó személyes adatok törlését. A Weltimmo azonban nem törölte ezeket az információkat, és kiszámlázta az érintetteknek a szolgáltatásainak díjait.[61] Az ügyben a szlovák adatkezelő szolgáltatása Magyarországra irányult, és ezzel az adatkezelő szolgáltatásban érintett ország hatóságának joghatósága vált kérdésessé. A NAIH bírságot szabott ki és az adatkezelési gyakorlatának megváltoztatására szólította fel az adatkezelőt. Joghatóságának meglétét azzal támasztotta alá, hogy az adatkezelő által végzett adatkezelés minden folyamata magyarországinak volt tekinthető. Az érintett cég vitatta a NAIH joghatóságát, és ezzel vitatta a kiszabott bírságot is, mert székhelye nem Magyarországon található.[62] Az eset az EUB elé került előzetes döntéshozatali eljárás keretében. Az eljárásban egyértelművé vált, hogy a természetes személyek védelme és a személyes adatok kezelése vonatkozásában[63] a formálisan más tagállam területén letelepedett adatkezelő esetén az alkalmazandó jog és a joghatósággal rendelkező felügyelő hatóság meghatározását, a felügyelő hatóság hatásköreinek gyakorlását és a szankcionálási jogkört az adatkezelő tevékenységi helye alapján ítélik meg. Az úgynevezett „egyablakos" eljárások esetében a Weltimmo-ügy már előrevetíti az érintett tagállami hatóság kiválasztási gyakorlatának egységesülését. A Weltimmo-ügy egyúttal hatással volt a GDPR-ban is megjelenő együttműködési és egységességi eljárások szabályaira, mivel a fő- és érintett felügyeleti hatóság kiválasztásának joghézagára mutatott rá.

A Hatóság 2018-as éves jelentéséből megtudható, hogy 2018-ban a magyar felügyeleti hatóság által az ún. Belső piaci információs rendszeren" keresztül fogadott ügyek jelentős része a GDPR 56. cikke szerinti, a fő- és érintett felügyeleti hatóságok azonosítására vonatkozó megkeresés volt. 2018. december 12-ig megközelítőleg 500 ilyen jellegű megkeresés érkezett a magyar hatósághoz. Az ügyeket a közösségi médiához, a keresőprogramokat üzemeltetőkhöz lehet kapcsolni, jellegük szerint az adatkezelés körülményeire vonatkozó tájékoztatás hiánya, törlési kérelmek elmaradása témakörben jelentősek. A Hatóság 2018 végéig 7 alkalommal kezdeményezett az 56. cikk szerinti eljárást.

2019-ben a Hatóság szintén „több száz" határon átnyúló ügyben vett részt. A Hatóság például releváns észrevételeket fogalmazott meg egy biztonsági szoftverekkel foglalkozó cég vírusirtójának ingyenes verziójának adatvédelmi beállításait vizsgáló ügyben,[64] ahol érintett hatóságként felhívta a holland fő hatóság figyelmét, ahová a panaszt benyújtották, hogy a fő felügyeleti hatóság döntésének tervezetében sem az eljárás tárgya, sem a jogkövetkezmények nincsenek megfelelően megjelölve. A Hatóság a NAIH/2019/2542. szerint érintett hatóságként járt el, és egy közelebbről meg nem nevezett nemzetközi bank adatkezelésének vizsgálatában vett részt, amely arra irányult, hogy a bank belső szabályaira hivatkozva 2 évig megőrizheti-e a pályázók önéletrajzát, ha a pályázó az adatainak törlését kéri. Az ügyben az Egyesült Királyság Adatvédelmi Biztos Hivatala volt a fő felügyeleti hatóság, mivel az adatkezelő központi ügyvitelének helye Londonban található.

2.4. A magyarországi adatvédelem szankcionálási és bírságolási gyakorlata

A szankcionálási és bírságolási gyakorlatot Magyarországon a NAIH és a bírói gyakorlat is befolyásolja. A bírságösszegeket áttekintve szintén a NAIH éves beszámolói állnak rendelkezésre, valamint 2020-as év adatai tárhatóak fel részben. Ezek alapján a 2015-ös évben 114,4 millió Ft, a 2016-os évben 20,2 millió Ft, a 2017-es évben 68,01 millió Ft, a 2018-as évben 40,236 millió Ft, a 2019-es évben 112,734 millió Ft és a 2020-as évben[65] ~148,204 millió Ft bírság került kiszabásra.

A bírságösszegek alakulására több tényező is kihat. Ilyen okból fakadóan a GDPR hatálybalépése előtti adatokat is érdemes figyelembe venni. A NAIH a korábbi évekhez képest jóval kevesebb esetben szabott ki bírságot a jogellenes adatkezelések miatt. Ennek oka, hogy a Kúria 2016-ban született jogerős ítélete szerint a Hatóságnak is alkalmaznia kell a kis- és középvállalkozásokról, fejlődésük támogatásáról szóló 2004. évi XXXIV. törvényt, mely szerint a kis- és középvállalkozások tekintetében első alkalommal elkövetett jogsértés esetén bírság kiszabása helyett figyelmeztetést kell alkalmazni.[66] A jogszabályi előterjesztés indoklásából kiderült, hogy a magyar jogalkotásnak szándéka volt védeni a magyar kkv-kat.

A GDPR hatálybalépése utáni első teljes egészében figyelembe vehető 2019-es év alapján is feltárhatóak bizonyos bírságolási gyakorlatot befolyásoló tényezők. 2019-ben két jelentősebb sajtóvisszhangot kiváltó ügy volt, az egyik a Sziget Zrt. NAIH/2019/55/5 ügyszámon nyilvántartott jogellenes adatkezelése (bírságösszeg 30 millió Ft).[67] A Sziget Zrt. ügyében a 2018. május 25. napját megelőzően végzett adatkezelés tekintetében, a Hatóság nem szabott ki bírságot, mert az Infotv. rendelkezéseit vette figyelembe, így a kis- és középvállalkozásokra vonatkozó rendelkezéseket is. A 2018. május 25. napjától végzett adatkezelés tekintetében viszont a Hatóság már úgy ítélte meg, hogy nem lenne elég visszatartó erő a figyelmeztetés, és közigazgatási bírságot is kiszabott a vállalkozásra. A másik eset a BRFK NAIH/2019/2471/6 ügyszámon nyilvántartott ügy az elveszett adathordozóval (*pendrive*-val) kapcsolatban (bírságösszeg 5 millió Ft). A BRFK tekintetében ki kell emelni, hogy a költségvetési szerv által elkövetett jogsértés miatt megállapítható bírság összegét százezer és húszmillió forint közötti összegben határozta meg a jogalkotó.[68] Utóbbi esetben a bírság kiszabása az incidens késedelmes bejelentése miatt történt, és indoklásában a Hatóság a GDPR Preambulumának (75) pontjára hivatkozott.[69]

2019-ben, a Hatóság honlapján elérhető 23 ügyszámot áttekintve, amelyek összesen 96 millió Ft bírságösszeget tartalmaztak, az éves beszámolóban közzétett 112 734 000 Ft bírságösszegből. Megállapítható, hogy 2019-ben a legalacsonyabb bírság összege 500 000 Ft volt, a legmagasabb összeg 30 millió Ft, és átlagban 4 173 913 Ft/ügy bírságot szabott ki a Hatóság. A bírságösszegek szórása 7 774 154 Ft volt.

2020-ban az összesen kiszabott bírságok összege ismét megemelkedett a korábbi évekhez képest, amelyre NAIH/2020/1160/10 ügyszámú határozata ad magyarázatot (Digi-ügy). A határozatból megállapítható, hogy a marasztalt ügyfelet két rendben is szabálysértőnek találták. A Hatóság megállapította, hogy: „Ügyfél megsértette a GDPR 5. cikk (1) bekezdésének b) (»célhoz kötöttség«) és e) (»korlátozott tárolhatóság«) pontjait, tehát a személyes adatok kezelésére vonatkozó elvek közül kettőt. Továbbá a GDPR 32. cikk (1)–(2) bekezdéseit, tehát az adatkezelés biztonságára vonatkozó részeket." A marasztalt ügyfél százmillió forintos bírságot kapott, amely magyarországi 2019-es árbevételének ~0,02%-a volt, a Hatóság a GDPR 83. cikke alapján értékelte az esetet. Ha a GDPR bírságolási szabályait nézzük, akkor az összeg messze elmarad a rendeletben megjelenő éves nettó árbevételen alapuló 2-4%-os bírságmértéktől. Kevésbé hangsúlyosan jelenik meg, hogy az ügyfelet nemcsak pénzbírságra kötelezte a NAIH, hanem arra is, hogy: „vizsgálja felül az általa kezelt valamennyi személyes adatokat tartalmazó adatbázist". Így a valóságos teher (szankció) lényegesen nagyobb lesz, mint az árbevétel 0,019%-a. Ha a GDPR-ban meghatározott 2%-ot vesszük alapul, és feltételezzük azt, hogy a NAIH ehhez próbált közelíteni, akár arra is lehet következtetni, hogy az adatvédelmi hatóság megközelítőleg egymilliárd forinttal „számolta" az adatbázisok átvilágításának költségét (2019-es árbevétel 1,91%-a). Elképzelhető persze, hogy a NAIH nem ezt a logikát követte, de az mindenesetre biztos, hogy a hatóság nemcsak bírságolással, hanem kötelező fejlesztések előírásával is hozzájárulhat a GDPR-ban foglaltak megvalósulásához, és ezeknek szintén jelentős költségvonzatuk lehet.

A bírság kiszabása a szankcionálási eszközök közül az egyik lehetőség, ahogy erre a GDPR és a kapcsolódó iránymutatás[70] is utal. A GDPR Preambulumának (148) pontja azt írja, hogy a „megfelelő intézkedéseken felül vagy azok helyett szankciókat – ideértve a közigazgatási bírságokat is – kell kiszabni". A szankciókiszabás esetén a GDPR a 83. és a 84. cikkben ad iránymutatást. A magyar szabályozásban az Infotv. rendelkezéseit érdemes megvizsgálni, összehasonlítva a GDPR követelményeit és a magyarországi szabályozást, felmerült egy jelentősebb kollízió.[71] Az Infotv. 75/A. §-a szerint a NAIH a GDPR 83. cikk (2)–(6) bekezdésében foglalt hatásköreit az arányosság elvének figyelembevételével gyakorolja, különösen azzal, hogy a személyes adatok kezelésére vonatkozó – jogszabályban vagy az Európai Unió kötelező jogi aktusában meghatározott – előírások első alkalommal történő megsértése esetén a jogsértés orvoslása iránt – a GDPR 58. cikkével összhangban – elsősorban az adatkezelő vagy adatfeldolgozó figyelmeztetésével intézkedik. E szakasz jogszabályba emelését a jogalkotó azzal indokolta, hogy a GDPR közvetlenül alkalmazandó szabályait elsősorban a tagállami jogrendszerek közötti különbséget kihasználó multinacionális gazdasági társaságok ellen fellépve szükséges alkalmazni, míg a többi gazdasági szereplő – elsősorban és kiemelten a magyar kis- és középvállalkozások – tekintetében a figyelmeztetés jogkövetkezménye indokolt.[72]

Több ügy vizsgálata alapján[73] elmondható, hogy a NAIH az Infotv. rendelkezéseit (75/A. §) és a GDPR-t [83. cikk (2)–(6) bek.] is figyelembe veszi. Ugyanakkor a magyar bírósági gyakorlatban megjelenik a 75/A. § alkalmazására való felhívás. A hatósági és a bírósági gyakorlatot össze kell egyeztetni, amellyel kapcsolatban a hatóság NAIH/2018/4283/2/V ügyszámon kiadott állásfoglalásában adott tájékoztatást. „A Hatóságot a bírságkiszabás vonatkozásában a Rendelet 83. cikkében foglaltak, *valamint* az Infotv. rendelkezései orientálják. […]". A Fővárosi Törvényszék 105.K.706.125/2020/12 ügyszámon lefolytatott eljárása és meghozott ítélete, amely egy közszereplő ügyében hozott határozat felülvizsgálatáról szóló perben született, indokolásában (dr. Hadházy Ákos Ányos ügye) is megerősíte-

ni látszik, hogy a bírságolás elmaradására nem minden esetben van lehetőség. A törvényszék az ítélet jogalapjáról szóló rész 42. pontjában kifejti, hogy a GDPR Preambulumának (148) pontjában, illetve az Infotv. 75/A. §-ában írtak nem értelmezhetőek kategorikus bírságtilalomként. Az ítélet indokolása szintén a 42. pontban kitér arra is, hogy a bírság maximuma lehetett volna 20 millió euró, amelyet pont a jövedelmi helyzet mérlegelése miatt nem alkalmazott a Hatóság. Egy másik ügyben, amely a 106.K.705.072/2020/6. ügyszám alatt a Hungária Med.M Kft. felperes ügyében a Fővárosi Törvényszék kifejtette, hogy az Infotv 75/A. §-a nem kötelező, csak iránymutatás. A Kúria a Kf.37998/2019/10. sz. ügyben[74] kimondta, hogy nincs olyan szabály, miszerint az első alkalommal történő jogsértés pusztán figyelmeztetéssel járna, és ehhez képest egyfajta kivétel lenne a bírságolás (DK honlap ügye).

Az ír tapasztalatokkal összevetve a magyar gyakorlat gyakrabban alkalmazza a bírság kiszabását, illetve hasonlóan megjelennek egyéb szankciók is. Utóbbiak adott esetben komolyabb terhet is jelenthetnek a megbírságolt fél számára, mint a közigazgatási bírság. Az eddigi tapasztalatok szerint a NAIH is rugalmasabbá teszi a hozzáállását, mivel „összetettebb és érzékenyebb megközelítés alkalmazására van szükség az adatkezelők és egyéb érdekeltek érdekeinek megértéséhez".[75]

Ahogy az ír példa rámutatott, a hatékony hatósági fellépés sok szempontból személyügyi tényezők függvénye is. A Hatóság személyi állománya 2015-ben 75 fő, 2016-ban 73 fő, 2017-ben 77 fő, 2018-ban 114 fő, 2019-ben megközelítőleg 105 fő volt. Az informatikus képzettség az elmúlt években felértékelődött, így a Hatóság jelentős kompetenciákért versenyez a munkaerőpiacon. Ruohonen és Hjerppe felmérték a magyarországi szakember-ellátottságot, és azt találták, hogy technikai szakemberek száma igen alacsony,[76] amely kihatással lehet a NAIH adatvédelmi incidenst felderítő és bizonyító képességére. Emellett a tapasztalt jogászoknak is nagyobb lett a mozgástere, mert magáncégek is keresik az adatvédelmi szakembereket.

3. Összegzés

Az uniós adatvédelmi szabályozás fejlődése elkerülhetetlenül összekapcsolódik a belső piac fejlődésével, valamint a technológiai változásokkal is. A sok esetben a belső piac egészét érintő online világ térhódítása, és a közösségi szolgáltatások és média előtérbe kerülése miatt már a GDPR előkészítésekor is felmerült annak a problémája, hogy miképpen lehet az uniós polgárnak és a piaci szereplőknek azonos szintű (adat)védelmet biztosítani, úgy, hogy az adatvédelmi szabályok végrehajtása szervezeti és eljárási szempontból tagállamonként eltér egymástól. A GDPR mint rendeleti formában megjelenő egységes uniós jogszabály komoly lépés az egységes joggyakorlat kialakításához. Az újonnan kialakított szabályozási koncepcióban megjelentek olyan elemek is, amely a több tagállamra kiterjedő adatvédelmi hatósági eljárások és a határon/határokon átnyúló adatkezelés dilemmáira adnak választ. Különös jelentőséget kapott ez a probléma a technológiai óriásvállalatok által nyújtott szolgáltatások és az adatkezelési jogsértések tömegessé válásával. Utóbbi tendenciák egyablakos, együttműködési és egységességi mechanizmusok kialakításával jártak együtt, amely a tagállami felügyeleti hatóságok mellett életre hívott az EAT formájában egy új szereplőt is. Utóbbi elsősorban a szabályozás egységes értelmezése, valamint az említett vitarendezés, egységes joggyakorlat kialakítása szempontjából jut főszerephez.

Az azonos védelem biztosításának alapja éppen az említett mechanizmusok és a tagállamok közötti együttműködés hatékonysága. Mind az ír, mind magyar hatósági tapasztalatok szerint a fenti mechanizmusok és együttműködési keretrendszer használata és alkalmazása megindult. Az ír példa alapján egyes hatóságok fellépése, szankcionálási hajlandósága kiemelkedően fontos lehet majd a későbbiekben az azonos szintű védelem biztosítása érdekében. Utóbbi szükségessé teheti a nem kellően szigorú hatósági hozzáállás felülvizsgálatát. Különösen igaz lehet az annak tükrében, hogy bizonyos jelek arra utalnak, hogy egyes technológiai óriásvállalatok a *forum shopping* eszközével élnének, hogy enyhébb szankcionálási gyakorlatot követő tagállami felügyeleti hatóságok joghatósága alá kerüljenek.

Másfajta tendencia is megmutatkozik, hiszen a bírságolás mellett a kapcsolódó szabályozás korrekciós intézkedések széles tárházát kínálja fel, amelyek alkalmazása mind az ír, mind a magyar gyakorlatban megindult. A későbbiekben érdemes lesz azt is megfigyelni, hogy a kiemelkedő nagyságú bírságösszegeken túl – egyfajta tagállamok közti „bírságlicitet" elkerülve – mely egyéb korrekciós intézkedések terjednek majd el a jogsértés/eset és a szankcionált fél egyedi körülményeire tekintettel. Ennek részeként a magyar gyakorlat azon dilemmája is tisztázódhat, hogy az uniós és tagállami rendelkezések együttes értelmezése alapján a bírságkiszabás mellett vagy helyett történjen meg figyelmeztetés adása – bár a legutóbbi idők is kiemelkedő összegű bírságok kiszabására nyújtanak újabb példákat. Az is egyértelmű már pár év tapasztalata alapján, hogy a hatékony hatósági fellépés egyik alapvető fontosságú tényezője a személyügyi és egyéb technikai feltételek megfelelő biztosítása tagállami szinten.

Jegyzetek

1 Guckelberger, Annette: Gibt es bald ein unionsrechtliches Verwaltungsverfahrensgesetz? Neue Zeitschrift für Verwaltungsrecht 2013/10. pp. 601–611.

2 Ezt az EuB esetjogában már korábban is elismerte (C-51-54/71. sz. ügy, International Fruit Company NV and others v Produktschap voor groenten en fruit, EU:C:1971:128, 4. pont; C-13/68, SpA Salgoil v Italian Ministry of Foreign Trade, EU:C:1968:54; C-179/84, Piercarlo Bozzetti v Invernizzi SpA and Ministero del Tesoro., EU:C:1985:306, 17. pont.)

3 Szegedi László: Az európai közigazgatás fejlődése és szabályozása. DialógCampus Kiadó, 2018. pp. 88–99.

4 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 [HL L 119., 2016.5.4., 1–88.] (a továbbiakban: GDPR)

5 Az Európai Parlament és a Tanács 95/46/EK 1995. október 24-i irányelve a személyes adatok feldolgozása vonatkozásában az egyének védelméről és az ilyen adatok szabad áramlásáról. [HL L 281., 1995.11.23., 31-50.] (a továbbiakban: 95/46/EK irányelv)

6 95/46 irányelv 29. cikke.

7 Amint azt a GDPR Preambulumának (124) és (125) pontjai kifejtik:
(124) Ha a személyes adatok kezelésére az adatkezelő vagy az adatfeldolgozó Unión belüli tevékenységi helyén folytatott tevékenységekkel összefüggésben kerül sor, és az adatkezelő vagy az adatfeldolgozó egynél több tagállamban rendelkezik tevékenységi hellyel, vagy ha az adatkezelő vagy az adatfeldolgozó kizárólag Unión belüli tevékenységi helyen folytatott tevékenységekkel összefüggésben megvalósuló adatkezelés az érintetteket egynél több tagállamban jelentős mértékben érinti vagy valószínűsíthetően jelentős mértékben érinti, akkor fő hatóságként az adatkezelő vagy az adatfeldolgozó tevékenységi központja vagy egyetlen tevékenységi helye szerinti felügyeleti hatósága jár el. A fő hatóság együttműködik olyan egyéb hatóságokkal, amelyek szintén érintettek amiatt, hogy az adatkezelő vagy adatfeldolgozó tevékenységi hellyel rendelkezik a tagállamuk területén, hogy a területükön lakóhellyel rendelkező érintettek jelentős mértékben érintve vannak, vagy, hogy panaszt nyújtottak be hozzájuk. Továbbá, ha az adott tagállam területén lakóhellyel nem rendelkező érintett nyújtott be panaszt, azt a felügyeleti hatóságot, amelyhez a panaszt benyújtotta, szintén érintett felügyeleti hatóságnak kell tekinteni. Az e rendelet (GDPR) alkalmazásával kapcsolatos kérdésekre vonatkozó iránymutatások kiadásával összefüggő feladatai keretében a Testület (EAT) számára lehetővé kell tenni, hogy iránymutatásokat adjon ki különösen azokra a szempontokra vonatkozóan, amelyeket figyelembe kell venni ahhoz, hogy meg lehessen győződni arról, hogy a szóban forgó adatkezelés egynél több tagállamban érint-e jelentős mértékben érintetteket, valamint arra vonatkozóan, hogy mi tekintendő releváns és megalapozott kifogásnak.
(125) Az e rendelettel összhangban rá ruházott hatáskörökkel élve, az intézkedésekre vonatkozó kötelező erejű döntések elfogadására a fő hatóság illetékes. A fő hatóságként eljáró felügyeleti hatóság a döntéshozatali folyamatba szorosan az érintett felügyeleti hatóságokat, és e folyamat során azokkal koordinál. Az érintett által benyújtott panasz részben vagy egészben történő elutasítására vonatkozó döntések esetében a döntést az a felügyeleti hatóság hozza meg, amelyhez a panaszt benyújtották.

8 Iránymutatás az adatkezelő vagy adatfeldolgozó fő felügyeleti hatóságának a meghatározásához (WP 244 rev.01).

9 GDPR 60–62. cikke.

10 GDPR 64. cikke.

11 GDPR 65. cikke.

12 GDPR 64. cikk (2) bekezdése.

13 Az elfogadott BCR-ek száma a NAIH éves beszámolóiban nem jelenik meg pontosan, de a NAIH az eljárások számának növekedését jósolja, 2019-ben két ilyen eljárás volt, 2020-as éves beszámolóban a NAIH pontos számot nem közölt.

14 Iránymutatás a 2016/679 rendelet szerinti közigazgatási bírság alkalmazásáról és megállapításáról (WP 253) pp. 5–6.
15 Dánia és Észtország jogrendszerében a felügyeleti hatóság kezdeményezésére a nemzeti bíróság rója ki a bírságokat (ld. Buzás Péter: 12. fejezet – Jogorvoslat, felelősség és szankciók a GDPR-ban. In: Péterfalvai Attila – Révész Balázs – Buzás Péter (szerk.): Magyarázat a GDPR-ról. Wolters Kulwer Kiadó, 2018, p. 365.).
16 Az Engel-kritériumokat az Emberi Jogok Európai Bírósága 1976-os Engel and Others v. The Netherlands (Application nos. 5100/71; 5101/71; 5102/71; 5354/72; 5370/72) ügyben hozott ítélete határozta meg. Ennek értelmében ahhoz, hogy eldöntsük, egy büntetőszankció büntetőjogi jellegű-e, három kritérium vizsgálata szükséges: az adott cselekmény büntetőjogi besorolása a nemzeti jogban, a rendelkezés természete és a büntetés jellege és súlya. A kritériumok közül a második kettő a lényeges, az első kizárólag csak kiindulópontként szolgál. Mivel az elrendelő hatóság nem játszik szerepet az intézkedés büntetőjogi voltának eldöntésében, így közigazgatási szankciók is büntetőjoginak tekinthetők. Ezért a *ne bis in idem* elv alapján egy jogerős közigazgatási szankció akár ki is zárhatja a későbbi büntetőeljárás megindítását. Lasagni, Giulia – Mirandola, Sofia: The European ne bis in idem at the Crossroads of Administrative and Criminal Law, Eucrim 2019/2. pp. 126–135.; Desterbeck, Francis: Ne bis in idem and Tax Offences: How Belgium Adapted its Legislation to the Recent Case Law of the ECtHR and the CJEU, Eucrim 2019/2. pp. 135–141.
17 Mateo, Fabio Pascua: Harmonising national sanctioning administrative law: An alternative to a single capital-markets supervisor, European Law Journal 2018/4-5. pp. 321–348.
18 GDPR (150) preambulumbekezdése.
19 GDPR (11) preambulumbekezdése.
20 Iránymutatás (WP 253), p. 6.
21 Iránymutatás (WP 253), pp. 6–8.
22 Iránymutatás (WP 253), p. 7.
23 Iránymutatás (WP 253), pp. 9–17.
24 Iránymutatás (WP 253), p. 9.
25 GDPR (148) preambulumbekezdés és 83. cikk (7) bekezdése.
26 Breach Notification Guidance Under The Data Protection Acts 1988–2003. https://www.dataprotection.ie/en/pre-gdpr/breach-notification-guidance-under-data-protection-acts-1988-2003 [2021.01.13.]
27 McLaughlin, Sharon: Ireland: A Brief Overview of the Implementation of the GDPR. European Data Protection Law Review 2018/2. pp. 228–229.
28 Breach Notification Guidance Under The Data Protection Acts 1988–2003. https://www.dataprotection.ie/en/pre-gdpr/breach-notification-guidance-under-data-protection-acts-1988-2003 [2021.01.13.]
29 McLaughlin i. m. pp. 231–233.
30 Bookman, Pamela K.: The Unsung Virtues of Global Forum Shopping, Notre Dame Law Review 2016/2. pp. 614–615.
31 Deloitte: Your move in the right direction – Investing in Ireland. https://www2.deloitte.com/content/dam/Deloitte/ie/Documents/Tax/IE_T_invest_in_ireland_0618_web_Draft1.pdf [2021.01.11.]; pp. 12–16.
32 Rodrigues, Clara Alves: „Digital Gangsters": Are Facebook and Google a Challenge to Democracy? Amsterdam Law Forum 2019/3. p. 34.
33 Vinocur, Nicholas: Millions of Americans rely on Europe's tough new privacy rules to safeguard their data, but the law's chief enforcer – Ireland – is in bed with the companies it regulates. POLITICO, 2019.04.24. Elérhető: https://www.politico.eu/interactive/ireland-blocks-the-world-on-data-privacy/ [2020.12.13.]
34 C-362/14. sz. ügy, Maximillian Schrems v. Data Protection Commissioner (Ireland), ECLI:EU:C:2015:650
35 Ivanics Krisztina: *A Schrems II. ítélet után – Az adatnak mennie kell.* Adatvedelmiszakerto.hu, 2020.09.18. Elérhető: https://www.adatvedelmiszakerto.hu/2020/09/a-schrems-ii-itelet-utan-az-adatnak-mennie-kell/ [2020.12.17.]
36 Bővebben lsd.: https://www.privacyshield.gov/welcome [2020.12.19.]
37 C-311/18. sz. ügy, Data Protection Commissioner (Ireland) v. Facebook Ireland Limited és Maximillian Schrems, ECLI:EU:C:2020:559
38 Ivanics Krisztina i. m.
39 C-498/16. sz. ügy, Maximillian Schrems v. Facebook Ireland Limited, ECLI:EU:C:2018:37
40 Lutzi, Tobias: 'What's a consumer?' (Some) clarification on consumer jurisdiction, social-media accounts, and collective redress under the Brussels Ia Regulation – Case C-498/16 Maximilian Schrems v. Facebook Ireland Limited, EU:C:2018:37. Maastricht Journal of European and Comparative Law, 2018/3., pp. 374-381.
41 Vinocur, Nicholas i. m.
42 Bookman, Pamela K.: i. m. p. 584.
43 Data Protection Commission of Ireland (IDPC): DPC Ireland 2018–2020 – Regulatory Activity under GDPR. 2020.06.24. Elérhető: https://www.dataprotection.ie/en/news-media/latest-news/dpc-ireland-2018-2020-regulatory-activity-under-gdpr [2020.12.19.]; pp. 8-11
44 Lsd.: https://dataprotection.ie/en/dpc-guidance/law/decisions-exercising-corrective-powers-made-under-data-protection-act-2018 [2020.12.29.]
45 GDPR 32. cikk (1) bekezdése; és 33. cikk (1) bekezdése.
46 GDPR 5.cikk (1) bekezdés d) pont; 32. cikk (1) és (4) bekezdés; és 33. cikk (1) bekezdés.
47 GDPR 5. cikk (1) bekezdés f) pont; és 32. cikk (1) bekezdés.
48 IDPC i. m. pp. 32–35.
49 GDPR 33. cikk (1) és (5) bek.
50 Lsd.: https://edpb.europa.eu/sites/edpb/files/decisions/final_decision_-_in-19-1-1_9.12.2020.pdf [2021.01.13.]
51 C-645/19. sz. ügy, Facebook Ireland and Others (ECLI:EU:C:2021:483) 96. pontja.
52 C-645/19. sz. ügy, Facebook Ireland and Others (ECLI:EU:C:2021:483) 53. pontja.
53 Lsd.: https://www.euractiv.com/section/data-protection/news/european-parliament-calls-for-infringement-procedure-against-ireland/ [2021.05.27.]
54 Tambou, Olivia: France: Lessons from the First Post-GDPR Fines of the CNIL against Google LLC, European Data Protection Law Review 1/2019, pp. 80–81.
55 Az alsó-szászországi adatvédelmi biztos 10,4 millió eurós bírságot szabott ki a notebooksbilliger.de részvénytársasággal szemben a munkavállalók jogszerűtlen megfigyelése miatt. https://lfd.niedersachsen.de/startseite/infothek/presseinformationen/lfd-niedersachsen-verhangt-bussgeld-uber-10-4-millionen-euro-gegen-notebooksbilliger-de-196019.html [2021.01.19.]. A hamburgi adatvédelmi biztos 35 millió eurós bírságot szabott ki a H&M ruházati társaság németországi szolgáltató központjára ugyancsak a munkavállalók jogszerűtlen megfigyelése miatt, amely anyag a megbírságolt társaságon belül elérhetővé is vált. https://datenschutz-hamburg.de/assets/pdf/2020-10-01-press-release-h+m-fine.pdf [2021.01.19.]
56 Ruohonen, Jukka – Hjerppe, Kalle: The GDPR Enforcement Fines at Glance, https://arxiv.org/abs/2011.00946 [2021.01.26], pp. 1–2.
57 Ruohonen, Jukka – Hjerppe, Kalle i. m. p. 2
58 Magyarország Alaptörvénye (2011. április 25.)
59 2011. évi CXI. törvény az alapvető jogok biztosáról.
60 Weltimmo s.r.o. kontra Nemzeti Adatvédelmi és Információszabadság Hatóság, NAIH1970/2013/H ügyszámon hozott határozata. https://www.naih.hu/files/1970_2013_hatarozat_anonim.pdf [2021.01.26]
61 C-230/14, Weltimmo s.r.o. kontra Nemzeti Adatvédelmi és Információszabadság Hatóság, ECLI:EU:C:2015:639.
62 C-230/14, Weltimmo s.r.o. kontra Nemzeti Adatvédelmi és Információszabadság Hatóság, ECLI:EU:C:2015:639. 25. pont és 41. pontjai.
63 GDPR 4 cikk (1) bekezdés, 28. cikk (1), (3) és (6) bekezdése.
64 A Nemzeti Adatvédelmi és Információszabadság Hatóság Beszámolója a 2019. évi tevékenységéről B/8988 p. 55
65 The GDPR Fines Report 2020. https://finbold.com/gdpr-fines-2020/ [2020.12.27.]
66 A Nemzeti Adatvédelmi és Információszabadság Hatóság Beszámolója a 2016. évi tevékenységéről B/13846. p. 54.
67 Sziget Kulturális Menedzser Iroda Zártkörűen Működő Részvénytársaság kontra Nemzeti Adatvédelmi és Információszabadság Hatóság, NAIH/2019/55/5 ügyszámon hozott határozat.
68 Buzás Péter i. m. p. 365.
69 Az ügy érdekessége, hogy későbbiek során az érintett szolgálati járművében megtalálták az elhagyott pendriveot, amihez illetéktelenek nem férhettek, így lehet úgy is értelmezni az esetet, hogy incidens nem is történt. Az eset rávilágít arra, hogy bírság kiszabása és az incidens valós hatásának értékelése időben eltérhet, így a bírság kiszabása után is kiderülhet, hogy az incidens fogalmi kritériumai nem állnak meg.
70 WP 253 iránymutatás a Rendelet szerinti közigazgatási bírság alkalmazásáról és megállapításáról (elfogadás időpontja: 2017. október 3.)
71 GDPR 2.0 konferencia: Péterfalvi Attila előadása https://www.portfolio.hu/uzlet/20180918/magyar-gdpr-birsag-nincs-kivetel-ha-sulyos-az-eset-298140 [2021.01.26] „A NAIH elnöke reflektált az Info tv. módosítás kapcsán a kkv-szektor tekintetében megjelent rendelkezésre és hangsúlyozta, hogy a bírságolás elmaradására nem minden esetben van lehetőség, hiszen az »elsősorban nem bírságol« kitétel nem jelent kötelezettséget, így súlyos gondatlanság, szándékosság, vagy gyermekek jogainak sérelme esetén a kkv-k sem kerülhetik el a bírságolást."
72 T/335. számú törvényjavaslat indokolással – az információs önrendelkezési jogról és az információszabadságról szóló 2011. évi CXII. törvény jogharmonizációs célú módosításáról
73 Példaként sorolva: „NAIH/2019/51/11. – „a Hatóság az általános adatvédelmi rendelet 83. cikk (2) bekezdése, az Infotv. 61. § (4) bekezdés b) pontja és az Infotv. 75/A. §-a alapján mérlegelte"; NAIH/2019/55/5. – „a Hatóság az általános adatvédelmi rendelet 83. cikk (2) bekezdése és az Infotv. 75/A. §-a alapján hivatalból mérlegelte az ügy összes körülményét"; NAIH/2019/133. – „a Hatóság az általános adatvédelmi rendelet 83. cikk (2) bekezdése és az Infotv. 75/A. §-a alapján hivatalból mérlegelte az ügy összes körülményét"; NAIH/2019/167/13. – […] A Hatóság hivatalból megvizsgálta, hogy indokolt-e a Kérelmezettekkel szemben adatvédelmi bírság kiszabása. E körben a Hatóság a GDPR 83. cikk (2) bekezdése és az Infotv. 75/A. §-a alapján mérlegelte az ügy összes körülményét, és megállapította, hogy a jelen eljárás során feltárt jogsértések esetében a figyelmeztetés se nem arányos, se nem visszatartó erejű szankció, ezért bírság kiszabása szükséges. […].
74 NAIH/2019/2668/2. számú határozatában megállapította, hogy a felperes nem tett eleget a természetes személyeknek a személyes adatok kezelése tekintetében történő védelméről és az ilyen adatok szabad áramlásáról
75 Jóri, András: Hungary: Introduction to the GDPR Application and a Brief History of Data Protection, European Data Protection Law Review 2019/4. sz. pp. 528–532; p. 532.
76 Ruohonen, Jukka – Hjerppe, Kalle i. m. pp. 1–2.