NEMZETI
KÖZSZOLGÁLATI EGYETEM
ÁLLAMTUDOMÁNYI ÉS NEMZETKÖZI TANULMÁNYOK KAR
CIVILISZTIKAI TANSZÉK

OPUSCULA IUVENUM EXCELLENTISSIMA

Rákos Dóra

A személyes adatok védelme az új európai adatvédelmi rendelet (GDPR) tükrében

2019/2.

1083 Budapest, Üllői út 82.| Tel: (1) 432-9000
Postai cím: 1519 Budapest, Pf.: 275.

Rákos Dóra[1]

A személyes adatok védelme az új európai adatvédelmi rendelet (GDPR) tükrében

1. BEVEZETÉS

„*NAGY TESTVÉR SZEMMEL TART!*” George Orwell 1984 című világhírű regényének szállóigévé vált mondata napjainkban talán aktuálisabb, mint valaha. Bár a könyvben lefestett disztópikus, elnyomás alatt lévő társadalom szerencsére csak távoli rémkép a legtöbb ember számára, az állandó megfigyelés veszélye a modern kor emberének sem ismeretlen fogalom. Az elmúlt évtizedek robbanásszerű technológiai fejlődésének, az internet térhódításának, az okostelefonok széleskörű elterjedésének következtében ugyanis a mindennapi életünk során ma már egyre többször kerülünk olyan helyzetbe, amikor valamilyen személyes jellegű információt gyűjtenek össze és tárolnak rólunk, a viselkedésünkről vagy a személyes preferenciáinkról. Személyes adataink egyaránt megtalálhatók az állami hatóságok, intézmények által vezetett nyilvántartásokban, valamint a különböző magánvállalkozások adatbázisaiban is, melyeket valamilyen jogszabályi kötelezettség vagy a saját gazdasági tevékenységük elősegítése érdekében hoztak létre.

A nyilvántartott személyes jellegű információk mennyiségének ugrásszerű növekedésével természetesen óhatatlanul együtt jár a személyes adatokkal való jogosulatlan visszaélések kockázatának emelkedése is. Sajnálatos módon az ilyen típusú jogsértések esetén – már pusztán a kezelt adatvagyon méretéből adódóan is – jellemzően rengeteg ember személyiségi jogai sérülnek. Gondoljunk csak például a közelmúlt legnagyobb visszhangot kiváltó esetére, a Cambridge Analytica botrányra, amikor a 2016-os amerikai elnökválasztás kampányidőszakában a Cambridge Analytica nevű elemző cég kb. 87 millió Facebook-felhasználó személyes adatait szerezte meg és használta fel az engedélyük nélkül politikai célokra. Az elmúlt években az ehhez hasonló visszaélések száma folyamatosan növekedett, ami jól mutatja, hogy az emberek egyre inkább elvesztik a kontrollt a személyes adataik felett.

Egy ilyen társadalmi-technológiai környezetben a megfelelő adatvédelmi szabályozásnak kulcsfontosságú szerepe van. Mindezt az európai jogalkotók is hamar felismerték, és a XX. század második felétől kezdve fokozatosan megteremtették a személyes adatok kezelésének jogi keretrendszerét. Ennek a folyamatnak a legújabb és talán a

[1] III. éves közigazgatás-szervező BA szakos hallgató, konzulens: Dr. Auer Ádám

legfontosabb mérföldkövének tekinthető az ún. általános adatvédelmi rendelet (*General Data Protection Regulation, GDPR*) bevezetése, amely révén megvalósult a személyes adatok védelmének európai szintű harmonizálása, egységesítése. A rendelet kétéves türelmi időszakot követően 2018. május 25-én lépett életbe, a közvélemény érdeklődésének középpontjába állítva ezzel az adatvédelmi szabályozás kérdéskörét.

Dolgozatomban a téma aktualitásánál fogva elsősorban arra a kérdésre keresem a választ, hogy napjaink információs társadalmában, a folyamatos technológiai és társadalmi változások közepette milyen eszközökkel kívánja biztosítani a jogalkotó a személyes adatok védelmét. A téma kifejtése során a GDPR előírásainak ismertetésén túl mind az európai, mind a hazai adatvédelmi szabályozás fejlődését bemutatom. Ennek kapcsán arra is igyekszem rávilágítani, hogy az új adatvédelmi rendelet korántsem előzmények nélküli, hanem jelentős mértékben épít a korábbi adatvédelmi szabályozásra.

Ami a szakdolgozatom szerkezeti felépítését illeti, először áttekintem az európai és a magyar adatvédelmi jog fejlődésének történetét, majd ismertetem a GDPR hatályba lépése előtti hazai szabályozás főbb jellemzőit. Ezt követően, dolgozatom központi részében az új európai adatvédelmi rendeletet veszem tüzetesebb vizsgálat alá. Ennek során egyrészt röviden összefoglalom a GDPR megalkotásának folyamatát, másrészt részletesen bemutatom a rendelet legfontosabb előírásait, kiemelt figyelmet fordítva arra, hogy a korábbi adatvédelmi szabályozáshoz képest milyen változásokat, újdonságokat hozott a rendelet. Az érintettek jogainak és az adatkezelők kötelezettségeinek ismertetése után arra is kitérek, hogy a jogalkotó milyen eszközöket biztosít a felügyeleti hatóságok számára a rendeletben foglalt szabályok kikényszerítéséhez. Végezetül összefoglalom a GDPR bevezetését követő időszak legfontosabb gyakorlati tapasztalatait, amelyeket uniós és hazai statisztikai adatokkal is igyekszem alátámasztani.

2. A SZEMÉLYES ADATOK VÉDELMÉNEK JOGI SZABÁLYOZÁSA

A személyes adatok védelmének vizsgálatát célszerű egy kissé távolabbról, a személyiségi jogok általános bemutatásával kezdeni. Ennek megfelelően először áttekintem a legfontosabb személyiségi jogokat, illetve a személyiségi jogok védelmére vonatkozó jogi szabályozásokat. Ezt követően térek rá a személyes adatok védelméhez való jog részletes elemzésére. Ennek keretében a szakirodalom alapján összefoglalom az adatvédelmi szabályozás fejlődését, kiemelve az egyes korszakok, generációk főbb jellemzőit. Emellett részletesen bemutatom a szabályozás európai, illetve hazai kialakulásának történetét, kiemelve a legfontosabb mérföldköveket. Végül a GDPR hatályba lépése előtti magyar szabályozás[2] alapján összefoglalom a személyes adatok védelméhez kapcsolódó legfontosabb alapfogalmakat, illetve a személyes adatok jogszerű kezelésének alapelveit. A jogszabály puszta ismertetésén kívül az értelmezéshez felhasználom a releváns hazai szakirodalmat is.

2.1. A személyiségi jogok védelmének általános bemutatása

A személyiségi jogokra – azok általános jellege miatt – nem adható egyértelmű definíció.[3] Hazánkban a személyiségi jogok védelmének jogszabályi keretrendszerét Magyarország Alaptörvénye biztosítja. Az Alaptörvény Szabadság és Felelősség című fejezetében leírja, hogy az ember sérthetetlen és elidegeníthetetlen alapvető jogait tiszteletben kell tartani. Az emberi méltóság sérthetetlensége magában foglalja többek között az egyén családi életének, magánéletének, otthonának és kapcsolati rendszerének tiszteletben tartását is. Ugyancsak az Alaptörvény tartalmazza, hogy az állampolgárokat megillető alapvető jogokat semmilyen magatartás tanúsításával nem lehet megsérteni.

A személyiségi jogok védelmének másik jogszabályi pillérét a 2013. évi V. törvény a Polgári Törvénykönyvről (továbbiakban: Ptk.) jelenti. A Ptk. szintén csak egy általános jellegű definíciót használ a személyiségi jogokra, amely az emberi méltósághoz való jog Alaptörvényben leírt fogalmára épül. A Ptk. tehát minden személyiségi jogot az emberi méltóságból eredeztet. Eszerint az emberi méltóságot és az abból fakadó személyiségi jogokat mindenki köteles tiszteletben tartani, különös tekintettel a magán- és családi élet, az otthon, a

[2] Az elemzéshez az Infotv. 2018 előtt hatályos változatát használtam fel, hogy a későbbiekben majd be tudjam mutatni a GDPR miatt bekövetkező változásokat.
[3] VÉKÁS – GÁRDOS (2014), 123.

másokkal való kapcsolattartás és a jóhírnév tiszteletben tartásához való jogra.[4] A Ptk. ezeket a jogokat általános jelleggel védelmezi, és az ezek megsértésére irányuló minden magatartási forma ellen védelmet nyújt.

A Ptk. a személyiségi jogok vonatkozásában egyfajta generálklauzulának tekinthető.[5] Ez azt jelenti, hogy az emberi méltóságból eredeztethető összes személyiségi jog a Ptk. védelme alatt áll, függetlenül attól, hogy külön nevesítésre kerültek-e a törvényben, vagy sem. Mindezt az Alkotmánybíróság gyakorlata is megerősíti, hiszen az több határozatában[6] is a következőképpen foglalta össze az általános személyiségi jog lényegét:

„Az általános személyiségi jog anyajog, azaz olyan szubszidiárius alapjog, amelyet mind az Alkotmánybíróság, mind a bíróságok minden esetben felhívhatnak az egyén autonómiájának védelmére, ha az adott tényállásra a konkrét, nevesített alapjogok egyike sem alkalmazható."

Ugyanezt az álláspontot képviseli Lenkovics Barnabás és Székely László[7] is. Meglátásuk szerint a személyiségi jogok védelmének legfőbb célja, hogy minden ember számára biztosítsa a háborítatlan, beavatkozástól mentes magán- és családi életet.

Bár a Ptk. inkább általános megközelítéssel él a személyiségi jogokkal kapcsolatban, néhány konkrét személyiségi jogot – köztük a dolgozatom témájául választott személyes adatok védelméhez való jogot – azonban külön is nevesít:[8] ezek a személyiségi jogok együttesen védik az emberek különböző érdekeit, mint például az egyén testi létét, a társadalomban való megítélését, az ott betöltött szerepét, a szabadságát, magánszféráját, valamint az egyén kegyeleti érzéseit, gyászát.

A személyiségi jogok általános jellegű definíciójából következik az is, hogy a Ptk.-ban a személyiségi jogok védelmét kimondó generálklauzulát már nem követi taxatív felsorolás, amely a személyiségi jogokat sértő magatartásokat tartalmazná. Így a törvény értelmében minden olyan cselekedet, amely korlátozza a másik ember emberi méltósághoz való jogát, jogsértőnek tekinthető. Fontos azt is megemlíteni, hogy ugyan az emberi méltóság mindenkit megillet, a személyiségi jogaink érvényesítése során azonban nem tanúsíthatunk olyan magatartást, amellyel más személy jogait bármilyen módon megsértenénk. Ebből adódóan

[4] Ptk. 2:42. §
[5] VÉKÁS – GÁRDOS (2014), 125.
[6] Például 8/1990. (IV. 23.) AB határozat, 470/B/2006. AB határozat, 192/2010. (XI. 18.) AB határozat
[7] LENKOVICS – SZÉKELY (2001), 100.
[8] Ptk. 2:43. §

minden ember köteles tartózkodni az olyan magatartásoktól, amelyek gátolhatják a másik embert abban, hogy emberi méltóságához méltó magatartást, életvitelt alakítson ki.[9]

2.2. Az európai adatvédelmi szabályozás fejlődése

Az előző fejezetben láthattuk, hogy a személyiségi jogok szorosan kapcsolódnak az egyén társadalomban betöltött szerepéhez. Ennek következtében a társadalmi körülmények változásával párhuzamosan a személyiségi jogok védelmének is újabb területei kerülnek előtérbe. Napjaink információs társadalmában, a technológia rohamléptékű fejlődésének eredményeképpen a személyes adatok védelméhez való jog a személyiségi jogok egyik legfontosabb elemévé, az állampolgárok alapvető jogává vált.

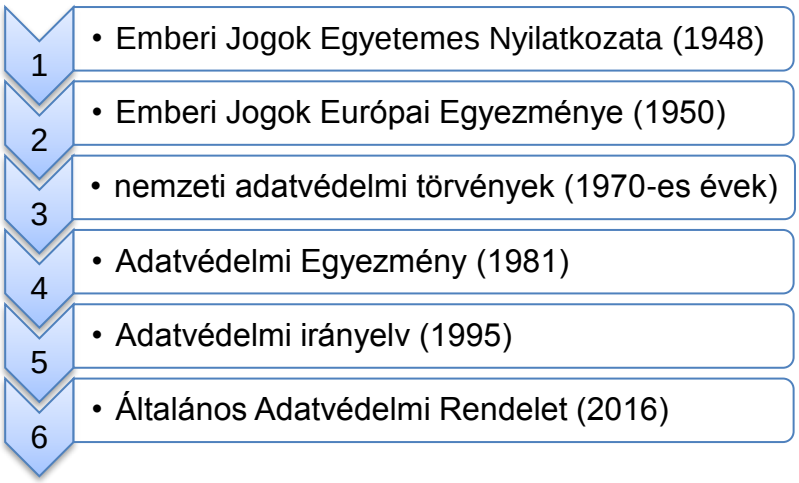
Az első generációs alapjogokkal (élethez, szabadsághoz való jog, stb.) ellentétben a személyes adatok védelme relatíve rövid múltra tekinthet vissza. Az adatvédelmi szabályozás kialakulásának kezdete a XX. század második felére tehető, ugyanis a számítástechnikai fejlődés következtében ekkor vált lehetővé, hogy az emberekről jóval több személyes jellegű információt gyűjtsenek össze és tartsanak nyilván.[10] Az ugrásszerűen megnövekedett adatmennyiség óhatatlanul szükségessé tette a személyes adatok védelmének szabályozását.

A meglehetősen rövid múlt ellenére az adatvédelmi szabályozás története több, egymástól viszonylag jól elkülöníthető korszakra, generációra osztható. A generációk számát illetően a szakirodalomban nincsen egységes álláspont, ugyanakkor a legtöbb szerző – többek között az első ilyen jellegű magyar tanulmányt publikáló Majtényi László[11] és az adatvédelem történetét szintén részletesen elemző Jóri András[12] is – az adatvédelmi jog három generációját különbözteti meg. Az első generációs szabályok az 1970-es években születtek meg, és az egyre szélesebb körben használt számítógépes nyilvántartások kapcsán fogalmaztak meg adatbiztonsági előírásokat. Az 1980-1990-es években megjelenő, második generációba tartozó joganyagok hatálya ezzel szemben már a papíralapú nyilvántartásokra is kiterjedt, emellett pedig a nemzetközi, határokon átnyúló adatáramlásokra vonatkozóan is tartalmaztak adatvédelmi szabályokat. Ezen generáció további jellemző vonása, hogy a jogalkotó nemcsak az adatkezelés megkezdése előtt, hanem annak teljes folyamata során is jogokat biztosított az adatalanyok számára.[13] Végül a harmadik generációs adatvédelmet az európai szintű

[9] VÉKÁS – GÁRDOS (2014), 126.
[10] SZŐKE (2014), 28-29.
[11] MAJTÉNYI (2003), 582-583.
[12] JÓRI (2009), 23.
[13] MAYER-SCHÖNBERGER (1997), 231.

szabályozás egységesítése, illetve a különböző iparágakra vonatkozó, speciális adatkezelési-adatvédelmi szabályok megjelenése jellemzi.

Az európai adatvédelmi szabályozás fejlődése jól követi az adatvédelmi generációk kapcsán korábban már ismertetett technológiai-társadalmi változásokat. A szabályozás történetének vizsgálatát azonban célszerű egy kissé korábbról kezdeni, hiszen az adatvédelem fogalma már a XX. század közepén megjelent a nemzetközi jogrendszerekben. Az egységes európai adatvédelmi szabályozás kialakulásához vezető legfontosabb jogi dokumentumokat az alábbi ábra szemlélteti:



1. ábra: Az egységes európai adatvédelmi szabályozás kialakulása

Bár az Egyesült Nemzetek Szervezete (ENSZ) által 1948-ban kiadott Emberi Jogok Egyetemes Nyilatkozata nem tartalmaz konkrét adatvédelmi szabályokat, a nyilatkozat mégis jelentős mérföldkőnek tekinthető, hiszen ez teremtette meg a személyiségi jogok védelmének általános keretrendszerét. Az Európa Tanács például ennek mintájára adta ki 1950-ben az Emberi Jogok Európai Egyezményét, amellyel az egyezményt aláíró országok kötelezettséget vállaltak az emberi jogok tiszteletben tartására.

Az első, kimondottan a személyes adatok védelmével kapcsolatos jogszabályok megjelenésére csak a következő évtizedekben, az egyre gyorsabb technológiai fejlődésre adott válaszlépésként került sor. A technológia és a számítástechnika fejlődése következtében ugyanis ekkor vált lehetővé a különböző (nagyrészt állami) nyilvántartásokban lévő adattömeg elektronikus rögzítése és tárolása. Ezzel párhuzamosan a digitalizált adatok védelme és az elektronikus adatfeldolgozás magánszférára gyakorolt hatása a társadalomelmélet képviselőit és a jogalkotókat is foglalkoztatni kezdte.[14] Ez vezetett el végül az 1970-es években az első,

[14] SZŐKE (2013), 109.

nemzeti szintű adatvédelmi törvények megalkotásához (pl. Svédország – 1973; NSZK – 1977; Dánia, Norvégia, Ausztria, Franciaország – 1978).[15]

Az első európai szintű, kizárólag az adatvédelemre koncentráló, jogilag kötelező erejű nemzetközi okmány kiadására csak pár évvel később, 1981-ben került sor.[16] Az Európa Tanács ugyanis ebben az évben fogadta el a 108. számú egyezményét[17], amellyel a számítógépes, automatizált nyilvántartásokkal szemben igyekeztek bizonyos mértékű védelmet biztosítani. Az egyezmény jelentőségét elsősorban az adta, hogy a nemzetközi jogban itt szerepelt először nevesítve a személyes adatok védelméhez való jog önállóan, mint a magánélethez való jog egyik megtestesülése.[18] Ezen túlmenően az egyezmény megalkotói külön figyelmet fordítottak a különleges adatok szigorúbb védelmére, a megfelelő szankciórendszer kialakítására és az adatbiztonság követelményére.[19]

Bár az adatvédelmi szabályozás területén közel másfél évtizedig az adatvédelmi egyezmény számított az egyetlen kötelező érvényű, nemzetközi szintű jogforrásnak, azonban az informatikai fejlődés, a személyi számítógépek egyre szélesebb körben történő elterjedése, a határon átnyúló adatáramlás volumenének folyamatos növekedése, valamint az adatok szabad áramlását megnehezítő, egymástól eltérő nemzeti szabályozások egy jóval átfogóbb, részletesebb szabályrendszer kidolgozását tették szükségessé. Ez vezetett el az európai adatvédelmi szabályozás következő jelentős állomásához, az 1995-ben kiadott, 95/46/EK számú adatvédelmi irányelvhez[20].

Az adatvédelmi irányelv igazi mérföldkövet jelentett a személyes adatok Európai Unión belüli védelmének történetében. Az irányelv megalkotása során két célt tartottak szem előtt: egyrészt a természetes személyek alapvető jogainak védelmét a személyes adatok feldolgozása vonatkozásában, másrészt pedig a személyes adatok tagállamok közötti szabad áramlásának elősegítését. Ezt a két, látszólag egymásnak kissé ellentmondó célt az irányelv úgy kívánta elérni, hogy a személyes adatok magas szintű védelmével elősegítse az adatok szabad áramlását nemcsak az Európai Unión belül, hanem harmadik országok vonatkozásában is.[21] Az irányelv

[15] Magyarországon az első adatvédelmi törvényt csak jóval később, 1992-ben alkotta meg az Országgyűlés.
[16] PÉTERFALVI (2012), 39.
[17] Európa Tanács (1981)
[18] SZIKLAY (2011), 63.
[19] SZŐKE (2014), 32.
[20] 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
[21] SZŐKE (2014), 44.

a korábbi adatvédelmi szabályokhoz képest mindenképpen jelentős előrelépést jelentett, melynek legfőbb újdonságai Jay és Hamilton[22] nyomán az alábbi pontokban foglalhatók össze:

1) az irányelv hatálya mind az automatizált, mind a manuális adatfeldolgozásra kiterjed,
2) az adatfeldolgozás jogszerűségére vonatkozó szabályok rögzítése,
3) külön előírások az érzékeny adatok kezelésére,
4) az érintettek jogainak meghatározása,
5) szigorúbb adatbiztonsági előírások az adatkezelés és -feldolgozás kapcsán,
6) a határon átnyúló adattovábbítások részletes szabályozása,
7) adatvédelemmel foglalkozó, 29. cikk szerinti munkacsoport létrehozása.

Az irányelv rendelkezéseit 1998-ig minden uniós tagállamnak kötelezően implementálnia kellett a saját nemzeti jogrendszerébe, így tulajdonképpen ez teremtette meg a harmonizált, európai szintű adatvédelmi szabályozás alapjait.[23] Az azóta eltelt mintegy két évtizedben bekövetkező technológiai-társadalmi változások miatt azonban szükségessé vált az adatvédelmi szabályozás koncepciójának teljes körű felülvizsgálata, melynek eredményeként 2016-ban elfogadásra került az új, általános adatvédelmi rendelet (*General Data Protection Regulation, GDPR*). A GDPR főbb jellemzőit, rendelkezéseit dolgozatom második felében fogom majd részletesen bemutatni.

2.3. A személyes adatok védelmének jogszabályi története hazánkban

Magyarországon – Európa többi részéhez hasonlóan – a XX. század második felében kezdődött az adatvédelmi szabályozás kialakulása. Első állomásának a Polgári Törvénykönyv 1977-es módosítása tekinthető[24], mely szerint „*A számítógéppel történő adatfeldolgozás nem sértheti a személyhez fűződő jogokat.*”[25] A törvényben emellett azt is rögzítették, hogy a nyilvántartott adatokról az érintett személyen kívül csak az arra jogosult szervnek vagy személynek lehet tájékoztatást adni. Az érintett személyt továbbá helyesbítési joggal ruházták fel, azaz amennyiben a nyilvántartásban szereplő valamely adat nem felelt meg a valóságnak, akkor az érintett kérhette a valótlan adat javítását, helyesbítését.

[22] JAY – HAMILTON (1999), 10.
[23] SZŐKE (2013), 110.
[24] PÉTERFALVI (2012), 50.
[25] 1977. évi IV. törvény a Magyar Népköztársaság Polgári Törvénykönyvéről szóló 1959. évi IV. törvény módosításáról és egységes szövegéről, 83. §

A személyes adatok alkotmányos védelmét az Alkotmány módosításáról szóló 1989. évi XXXI. törvény hozta el, amely hazánkban elsőként határozta meg alapvető emberi jogként a személyes adatok védelmét:[26]

„59. § A Magyar Köztársaságban mindenkit megillet a jóhírnévhez, a magánlakás sérthetetlenségéhez, valamint a magántitok és a személyes adatok védelméhez való jog."

A személyes adatok védelmének alapvető emberi jogként való megjelenése ugyan jelentős lépés volt, a jogszabály azonban nem adott részletes definíciót arra vonatkozóan, hogy a szabályozó pontosan mit is ért a személyes adatok védelme alatt. A jogelv gyakorlatban való értelmezése tehát nem volt egyértelmű, melynek következtében több alkalommal is az Alkotmánybíróság állásfoglalására volt szükség.[27] Az Alkotmánybíróság 15/1991. (IV. 13.) AB határozata például megsemmisítette a népesség-nyilvántartásra és a személyes adatok kezelésére vonatkozó korábbi rendelkezések egy részét, mivel azok sértették a személyes adatok védelméhez való jogot. Ez a határozat egyébként abból a szempontból is kiemelt jogtörténeti jelentőséggel bírt, hogy számos olyan, a személyes adatok védelmével kapcsolatos jogintézményt (pl. adatkezelés célhoz kötöttsége) teremtett meg, amelyek a mai napig az adatvédelmi szabályozás alapját képezik.[28]

Ezen előzmények után alkotta meg az Országgyűlés az 1992. évi LXIII. törvényt a személyes adatok védelméről és a közérdekű adatok nyilvánosságáról (továbbiakban: Avtv.), amely hazánk első adatvédelmi törvénye volt. Bár Európa nagy részében az első nemzeti adatvédelmi törvények már az 1970-es években, az első generációs adatvédelmi szabályozás korszakában megjelentek, a hazai adatvédelmi törvény a második generációs adatvédelmi jogalkotás vonásait tükrözi. Ennek megfelelően az Avtv. hatálya mind a számítógépes, mind a manuális adatkezelésre kiterjedt. Fontos még megemlíteni, hogy a törvény a személyes adatok védelméhez fűződő alkotmányos jog általános szabályozásán kívül a közérdekű adatok nyilvánosságáról és az adatvédelmi biztos pozíciójának létrehozásáról is rendelkezett.[29]

Az 1992-es adatvédelmi törvényt az információs önrendelkezési jogról és a közérdekű adatok nyilvánosságáról szóló 2011. évi CXII. törvény (továbbiakban: Infotv.) váltotta fel. Az Infotv. tulajdonképpen megőrizte az adatvédelmi szabályozás korábbi rendszerét, habár néhány helyen kiegészítette, pontosította a kapcsolódó szabályokat. Az Infotv. egyik legfontosabb újítása a Nemzeti Adatvédelmi és Információszabadság Hatóság (NAIH) létrehozása volt. A

[26] PÉTERFALVI (2012), 50.
[27] MAJTÉNYI (2006), 168-175.
[28] PÉTERFALVI (2012), 51.
[29] JÓRI – HEGEDŰS – KEREKES (2010), 35.

NAIH autonóm közigazgatási szervként egyrészt átvette az adatvédelmi biztos korábbi feladatait, másrészt további hatáskörökkel (pl. bírságolási jog) is felruházták.[30] Hazánkban a személyes adatok védelmét azóta is az Infotv. szabályozza, bár a GDPR bevezetésével a jogharmonizációs kötelezettségnek eleget téve az Infotv. is módosításra került.[31]

2.4. A személyes adatok védelmével kapcsolatos alapfogalmak, alapelvek

A személyes adatok védelméhez kapcsolódó legfontosabb fogalmakat az Infotv. tartalmazza. Bár a törvény számos alapfogalmat részletekbe menően definiál, érdekes módon magának a személyes adatok védelmének a fogalmát nem határozza meg egyértelműen. Emiatt a szakirodalomban többféle meghatározással is lehet találkozni a személyes adatok védelmére vonatkozóan. A Nemzeti Adatvédelmi és Információszabadság Hatóság (NAIH) szerint például a személyes adatok védelme alatt a személyes adatok jogszerű kezelését, az érintett személyek védelmét biztosító alapelvek, szabályok, eljárások, adatkezelési eszközök és módszerek összességét kell érteni.[32] Ez a meghatározás elsősorban a személyek védelmét tartja szem előtt, míg az adatok kapcsán csak a jogszerű kezelést írja elő.

Majtényi László, korábbi adatvédelmi biztos hasonló megközelítéssel él. Meghatározása szerint[33] ugyanis a személyes adatok védelme nem magának az adatnak a védelmét jelenti, hanem sokkal inkább az egyén, az adatalany védelmét kell biztosítania. Majtényi definíciója azért is érdekes, mert felhívja a figyelmet arra az ellentmondásra, hogy bár az adatvédelem kifejezés szó szerinti értelmezésben az adatok védelmét jelenti, a valóságban azonban nyilvánvaló módon az adatalany személyének védelmét értjük alatta. A szerző érdekességképpen azt is megemlíti, hogy az adatvédelem mint kifejezés hasonlóképpen jelenik meg a világ számos másik nyelvében is (pl. *data protection, Datenschutz, protection des données*). Mindezek alapján meglátása szerint az adatok védelmére inkább az adatbiztonság kifejezést lenne célszerű használni.

Jóri András Majtényihoz hasonlóan a magánszféra védelmének szempontjából értelmezi a személyes adatok védelmét. Definíciója szerint *„az adatvédelem minden esetben a*

[30] PÉTERFALVI (2012), 55.
[31] 2018. évi XXXVIII. törvény az információs önrendelkezési jogról és az információszabadságról szóló 2011. évi CXII. törvénynek az Európai Unió adatvédelmi reformjával összefüggő módosításáról, valamint más kapcsolódó törvények módosításáról
[32] NEMZETI ADATVÉDELMI ÉS INFORMÁCIÓSZABADSÁG HATÓSÁG (2018A)
[33] MAJTÉNYI (2006), 63.

személy magánszférájának jogi védelmét jelenti".[34] Emellett azt is kiemeli, hogy a személyes adatok védelme folyamatosan változik, követve a leginkább a technológiai fejlődés által előidézett adatvédelmi kihívásokat. Jóri egy másik munkájában[35] ezenkívül felhívja a figyelmet az adatvédelem és adatnyilvánosság elve közötti ellentmondásra is, melyeknek ideális jogi környezetben egyensúlyban kell lenniük.

A fentiekkel ellentétben az Infotv. a személyes adatok védelméhez való jog helyett az információs önrendelkezés jogát és az információszabadságot állítja a szabályozás középpontjába. Az információs önrendelkezés joga – a személyes adatok védelméhez való joghoz hasonlóan – az Alaptörvény VI. cikkén alapszik. A két fogalom azonban nem ekvivalens egymással: bár az információs önrendelkezési jog szorosan kapcsolódik az adatvédelemhez, annál bizonyos szempontból szűkebb kategóriának tekinthető. Az információs önrendelkezési jog jogosultságot biztosít a természetes személyek számára, hogy személyes adataikról, a rájuk vonatkozó információk nyilvánosságra hozataláról saját maguk rendelkezhessenek.[36] Ezzel szemben az adatvédelem kérdéskörébe – az információs önrendelkezési jog biztosításától függetlenül – beletartozik az összes olyan szabályozás, amely az egyén személyes adatainak kezeléséhez kapcsolódik.[37] Az adatvédelmi jog így például magában foglalja az adatbiztonság követelményét is. Ugyanakkor vannak olyan kötelező adatszolgáltatások (pl. népszámlálás), melyek során az állampolgárok önrendelkezési joga háttérbe szorul, míg az adatvédelmi és adatbiztonsági szabályozás ugyanúgy érvényesül ezekben az esetekben is.[38]

Az Infotv. ugyan a személyes adatok védelmének fogalmát konkrétan nem határozza meg, ám az ehhez kapcsolódó alapfogalmakat (pl. személyes adat, érintett, stb.) már részletesen ismerteti. A személyes adatnak két fontos elemi része van: az adat és az érintett. A törvény által leírt fogalmakat nézve figyelemreméltó, hogy az adat fogalmának meghatározását nem tartotta fontosnak a jogalkotó. A személyes adat fogalmából azonban ki lehet következtetni az adat definícióját is: ez alapján adatnak minősül minden olyan ismeret, amely a mindennapok során az állampolgárok tudomására jut, vagyis a konkrét tények és információk mellett adatnak minősülnek az ezen ismeretekből levont következtetések, vélemények is.[39]

Másik fontos elemi fogalom az érintett, amelynek definícióját a korábbi adatvédelmi törvény (Avtv.) nem tartalmazta. Az Infotv. 3. § 1. pontja szerint érintettnek számít bármely

[34] JÓRI (2005), 17.
[35] JÓRI (2006), 109-110.
[36] 15/1991. (IV. 13.) AB határozat
[37] JÓRI – SOÓS (2016), 22.
[38] MÉSZÁROS (2017), 22-23.
[39] PÉTERFALVI (2012), 59.

információ alapján azonosított vagy azonosítható természetes személy. Az érintett tehát az a személy, akire vonatkozóan olyan információ áll rendelkezésre, amely alapján az adott személy közvetlenül vagy közvetve azonosítható. A törvény által alkalmazott definícióból emellett az is következik, hogy a jogi személyek adatai nem minősülnek személyes adatnak.

A személyes adat és az érintett fogalmán kívül a törvény még számos lényeges fogalmat definiál az adatvédelemmel kapcsolatosan (pl. különleges adat, hozzájárulás, adatkezelés, adatfeldolgozás, stb.). A különleges adatok közé sorolhatók többek között a faji eredetre, a nemzetiséghez való tartozásra, a vallásra, az egészségi állapotra, illetve a káros szenvedélyekre vonatkozó adatok. Ezeket az információkat „érzékenységükre" való tekintettel kifejezetten magas fokú védelemben kell részesíteni, ezért ezen adatok csak a törvényben meghatározott feltételek (pl. állampolgárok érdekeinek védelme, nemzetbiztonság, bűncselekmények megelőzése, felderítése, stb.) esetén kezelhetőek.

A személyes adatok kapcsán különösen nagy figyelmet kell fordítani arra, hogy a legtöbb esetben az érintett személy hozzájárulását kell kérni, hogy a rá vonatkozó adatokat az adatkezelő kezelhesse.[40] Az érintett által adott hozzájárulásnak három elengedhetetlen feltételnek kell megfelelnie: önkéntesség, egyértelműség és tájékozottság.[41] Az első kritérium értelmében a hozzájárulásnak mindig önkéntesnek kell lennie, vagyis tilos az érintett személy hozzájárulását valamilyen hátrány kilátásba helyezésével kikényszeríteni. Másik fontos követelmény az egyértelműség, azaz a hozzájárulásból egyértelműen következnie kell, hogy az érintett beleegyezik az adatkezelésbe. Az érintett hozzájárulásához emellett nélkülözhetetlen az adatkezelő részéről történő megfelelő tájékoztatás is, amelynek tartalmaznia kell az adatkezelés minden lényeges elemét (pl. adatkezelést végző személy, adatkezelés célja, stb.). A hozzájárulás megtételére az Infotv. csupán a különleges adatok esetében követeli meg az írásbeliséget, más típusú adatok esetén a hozzájárulás történhet szóban, illetve ráutaló magatartással is. Fontos még megemlíteni, hogy az érintett az adatkezelés során a hozzájárulását bármikor, egyszerű módon, külön indoklás nélkül visszavonhatja.

A személyes adatok védelme kapcsán az egyik legkritikusabb terület az adatok kezelése és feldolgozása. Az adatkezelés az Infotv. 3. § 10. pontja értelmében magában foglal minden olyan tevékenységet, amely során személyes adatokon vagy éppen azokkal végeznek valamilyen műveletet. Ebbe a kategóriába sorolható többek között az adattovábbítás, adattörlés,

[40] Ez alól csak a jogszabály által elrendelt, közérdekű célt szolgáló adatkezelések jelentenek kivételt. Ebben az esetben ugyanis az érintett kifejezett hozzájárulása nélkül is kezelhetőek a személyes adatok. [Infotv. 5. § (1) bekezdés]
[41] PÉTERFALVI (2012), 65-66.

adatzárolás és az adatmegsemmisítés is. Ezen feladatok koordinálását az adatkezelő végzi, vagyis ő határozza meg, hogy milyen adatok szükségesek az adott feladat végrehajtásához, valamint irányítja és felügyeli az adatfeldolgozó tevékenységét is. Az adatfeldolgozó személye abban különbözik az adatkezelőtől, hogy az adatkezelő utasításai szerint ő végzi el azokat a technikai adatkezelési műveleteket, amelyek érdemi döntést már nem igényelnek (pl. adatrögzítés, adatok archiválása).[42]

Az Infotv. az alapfogalmak magyarázatát követően, a 4. §-ban részletesen kifejti a személyes adatok kezelésének alapelveit. Ezek olyan követelmények, amelyekre az adatkezelőnek az adatkezelés teljes folyamata során tekintettel kell lennie. Az egyik legfontosabb adatkezelési alapelv – a törvényesség és a tisztesség elvén kívül – a célhoz kötöttség, melyet már a korábbi adatvédelmi törvény is előírt. A célhoz kötöttség elve alapján személyes adatot csak pontosan meghatározott, jogszerű céllal lehet kezelni. Az adatkezelés céljának meghatározásán kívül annak jogszerűsége is elengedhetetlen. Ebből adódóan az adatkezelésnek indokoltnak kell lennie társadalmi szempontból, azaz személyes adat kezelését kizárólag valamilyen jog érvényesítése vagy kötelezettség teljesítése céljából lehet végezni.[43]

Egy másik lényeges alapelv az adatminimalizálás (vagy más néven adattakarékosság) elve: az Infotv. 4. § (2) bekezdése értelmében kizárólag azok a személyes adatok kezelhetőek, amelyek az adatkezelés céljának megvalósulásához nélkülözhetetlenek. További fontos kritérium, hogy ezek az adatok kizárólag az adott cél eléréséhez szükséges mértékben és ideig használhatóak fel. Az adatminőség elvének értelmében pedig az adatkezelések során emellett biztosítani kell a személyes adatok pontosságát, teljességét, naprakészségét is.[44]

Az adatkezelés elvei közé tartozik a helyreállíthatóság követelménye is. Az Infotv. 4. §-ának (3) bekezdése szerint a személyes adat mindaddig megőrzi a minőségét, amíg az adat és az érintett személy közötti kapcsolat helyreállítható. Jóri[45] megkülönbözteti a helyreállíthatóság abszolút és relatív értelmezését. Az abszolút értelmezés szerint egy adat már akkor is személyes adatnak minősül, ha van olyan személy, aki az alapján egyértelműen be tudja azonosítani az érintettet. A hazai joggyakorlat ezzel szemben a relatív megközelítést alkalmazza, mely szerint csak azok az adatok tekinthetők személyes adatnak, amelyek alapján az adatkezelő képes kapcsolatot találni az adott adat és az érintett személy között.

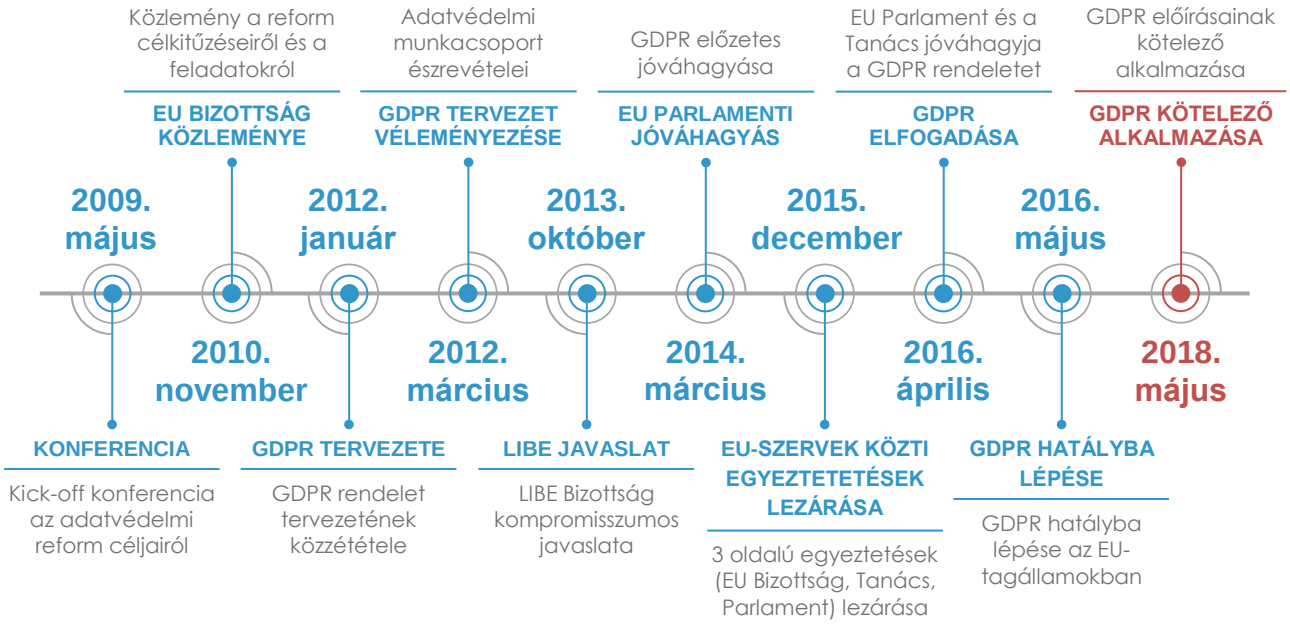
[42] Infotv. 3. § 18-19. pont
[43] PÉTERFALVI (2012), 74.
[44] Infotv. 4. § (4) bek.
[45] JÓRI (2010), 39-40.

3. AZ EURÓPAI ADATVÉDELMI RENDELET (GDPR) BEMUTATÁSA

Az 1995. évi adatvédelmi irányelv megalkotásával – mintegy fél évszázadnyi jogrendszeri fejlődés eredményeként – többé-kevésbé sikerült Európában egy egységes, harmonizált, a különböző országok adatvédelmi megközelítéseit összhangba hozó és azokat továbbfejlesztő adatvédelmi szabályrendszert kialakítani. Az irányelv elfogadása óta ugyanakkor a globalizáció új szintre emelkedett, és az információs technológiában sosem látott mértékű fejlődés következett be (pl. számítógépek és internethasználat tömeges elterjedése, közösségi oldalak térnyerése, okostelefonok megjelenése, elektronikus fizetési rendszerek széleskörű használata). Az Európai Unió jogalkotó szervei a 2000-es évek végére felismerték, hogy az adatvédelmi irányelv már nem képes a technológiai-társadalmi változásokkal lépést tartani, az újonnan felmerülő kihívásoknak megfelelni. Emiatt elkerülhetetlenné vált a korábbi szabályozás felülvizsgálata és alapvető újragondolása, így a szabályalkotók az adatvédelmi szabályozás átfogó reformjaként egy új jogszabály, az Általános Adatvédelmi Rendelet (*General Data Protection Regulation, GDPR*) megalkotására tettek javaslatot.

3.1. A GDPR megalkotásának folyamata

Az új adatvédelmi szabályrendszer hosszas, több évet átölelő előkészítő munka eredményeként született meg. A személyes adatok Európai Unión belüli védelmével kapcsolatos jogi keretrendszer felülvizsgálata és az új koncepció kidolgozása már 2009 májusában, egy magas szintű kick-off konferencián elkezdődött.



2. ábra: A GDPR megalkotásának folyamata

Az adatvédelmi reform legfontosabb célkitűzéseit 2010 novemberében, közlemény[46] formájában hozta nyilvánosságra az Európai Bizottság. A jogalkotó a közleményben arra a következtetésre jutott, hogy az Európai Uniónak átfogóbb és következetesebb politikára van szüksége annak érdekében, hogy a személyes adatok védelme tekintetében meg tudjon felelni az új kihívásoknak, valamint hogy garantálni tudja az uniós állampolgárok adatvédelemhez fűződő alapvető jogait az EU határain belül és azokon túl is.

A Bizottság hosszas előkészítő munka után 2012. januárban hozta nyilvánosságra az új adatvédelmi szabályrendszer, az általános adatvédelmi rendelet tervezetét.[47] A reformcsomag talán legszembetűnőbb vonása maga a jogi forma, hiszen a jogalkotó a korábbi irányelv módosítása helyett a rendeleti formában történő szabályozás mellett döntött. Ennek oka, hogy utóbbival egy olyan, minden tagállamban közvetlenül hatályos jogforrás szabályozza majd az adatvédelem kérdéskörét, amely megszünteti a tagállamok helyenként eltérő jogi megközelítéseit, és egyúttal megteremti az egységes európai adatvédelmi szabályozást.

A rendelettervezet kapcsán még számos észrevétel, módosító javaslat érkezett, így a jogalkotási folyamat következő lépéseként háromoldalú egyeztetések kezdődtek az általános adatvédelmi rendelet tervezetéről az Európai Bizottság, az Európai Unió Tanácsa és az Európai Parlament között. A három intézmény végül 2015. decemberben állapodott meg az új

[46] Európai Bizottság (2010)
[47] Európai Bizottság (2012)

jogszabály végleges szövegében, amelyet az Európai Unió Tanácsa és az Európai Parlament 2016 áprilisában fogadott el. Ennek eredményeként kihirdették az Európai Parlament és a Tanács (EU) 2016/679 számú rendeletét[48], amely 2016. május 24-én lépett hatályba. Az új, Általános Adatvédelmi Rendelet (*General Data Protection Regulation, GDPR*) néven kiadott jogszabály hatályba lépésével egyúttal a 95/46/EK irányelvet is hatályon kívül helyezték. A rendeletben foglaltak alkalmazására kétéves türelmi időszak állt rendelkezésre, így a GDPR előírásait csak 2018. május 25-től kell közvetlenül alkalmazniuk a tagállamoknak.

3.2. A GDPR részletes bemutatása

Az adatvédelmi szabályozás történetében kétségkívül az általános adatvédelmi rendelet jelenti az eddigi legátfogóbb, legrészletesebb joganyagot. A szabályozás teljes körű, minden részletre kiterjedő bemutatása sajnos azonban meghaladná a szakdolgozat terjedelmi korlátait. Éppen ezért dolgozatom következő részében leginkább a GDPR által bevezetett újdonságok ismertetésére törekszem, kiemelve a főbb eltéréseket a korábbi szabályozáshoz képest.

3.2.1. A rendelet hatálya

A GDPR rendelkezéseinek elemzését célszerű a rendelet tárgyi és területi hatályának bemutatásával kezdeni. A rendelet tárgyi hatálya a korábbi irányelvhez képest nem változott, a 2. cikk (1) bekezdése értelmében egyrészt kiterjed a személyes adatok bármely formában történő automatizált kezelésére, másrészt a manuális, nem automatizált adatkezelések azon részére is, amelyek során személyes adatokat nyilvántartási rendszerekben tárolnak. Bár a GDPR hatálya a manuális adatkezelések esetében kizárólag a strukturált adattárolásokra korlátozódik, a magyar jogalkotó az Infotv. hatályát a manuálisan végzett adatkezelések minden formájára kiterjesztette.[49] Ugyanakkor a természetes személyek magáncélú, otthoni tevékenység keretében végzett adatkezelése (pl. rokonok születésnapjának, ismerősök telefonszámának nyilvántartása) nem tartozik a rendelet hatálya alá.[50]

[48] Az Európai Parlament és a Tanács (EU) 2016/679 rendelete 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 (általános adatvédelmi rendelet)
[49] JÓRI – SOÓS (2016), 91-92.
[50] A kizárólag személyes célt szolgáló adatkezelések törvény alóli mentesítéséről már az Infotv. is rendelkezett a GDPR bevezetését megelőzően [Infotv. 2. § (4) bek.]

A tárgyi hatályhoz képest a rendelet területi hatályát már egy kissé bonyolultabban határozta meg a jogalkotó. A rendelet 3. cikke értelmében ugyanis a GDPR területi hatálya alá alapvetően a személyes adatok kezelésének alábbi esetei tartoznak:

1) az EU-ban tevékenységi hellyel rendelkező adatkezelők vagy adatfeldolgozók adatkezelése (függetlenül attól, hogy az adatkezelés az EU területén történik-e vagy sem)
2) az EU-ban tevékenységi hellyel nem rendelkező adatkezelők vagy adatfeldolgozók adatkezelése, amennyiben az érintett az Unióban tartózkodik, és az adatkezelés:
    a) áruknak vagy szolgáltatásoknak az Unióban tartózkodó érintettek számára történő nyújtásához kapcsolódik, vagy
    b) az érintett Unión belül tanúsított viselkedésének megfigyelésére irányul

A területi hatály kapcsán alapvetően két tényezőt kell mérlegelni: az adatkezelő vagy adatfeldolgozó tevékenységi helyét, valamint az adatkezelés érintettjének tartózkodási helyét. Ebből következik, hogy a GDPR szempontjából egyaránt irreleváns az érintett állampolgársága, az adatkezelő/adatfeldolgozó központjának helye, illetve az adatkezelési tevékenység tényleges helyszíne is. Ennek megfelelően a rendelet hatálya kiterjed arra az esetre is, amikor az EU-ban tevékenységi hellyel rendelkező cég az Unión kívül végzi harmadik országbeli állampolgárok személyes adatainak kezelését.[51] Ezzel szemben, például ha egy Brazíliában tartózkodó, uniós tagállam állampolgárjáról egy EU-ban tevékenységet nem folytató vállalat személyes adatokat rögzít az érintett ottléte során, akkor a cég adatkezelési tevékenységére nem kell a GDPR előírásait alkalmazni. A GDPR területi hatályának értelmezéséhez a következő táblázat nyújt segítséget:

Érintett állampolgársága	Érintett tartózkodási helye	Adatkezelő/adatfeldolgozó tevékenységi helye*	GDPR hatálya alá tartozik?	
			Igen / Nem	Ha igen, akkor melyik pont alapján
EU	EU	EU	✓	3. cikk / 1. pont
EU	EU	Nem EU	✓	3. cikk / 2. pont**
EU	Nem EU	EU	✓	3. cikk / 1. pont
EU	Nem EU	Nem EU	✗	
Nem EU	EU	EU	✓	3. cikk / 1. pont
Nem EU	EU	Nem EU	✓	3. cikk / 2. pont**
Nem EU	Nem EU	EU	✓	3. cikk / 1. pont
Nem EU	Nem EU	Nem EU	✗	

1. táblázat: A GDPR területi hatályának áttekintése

Megjegyzések:
* Ez az oszlop azt jelzi, hogy az adatkezelő/adatfeldolgozó rendelkezik-e EU-n belüli tevékenységi hellyel.
** Ezen eseteknél azt feltételeztem, hogy az adatkezelési tevékenység áru/szolgáltatás nyújtásához kapcsolódik vagy az érintett Unión belül tanúsított viselkedésének megfigyelésére irányul.

[51] JÓRI – SOÓS – BÁRTFAI – HÁRI (2018), 110.

3.2.2. Alapfogalmak

Az általános adatvédelmi rendeletben foglalt részletszabályok értelmezéséhez elengedhetetlen az adatvédelemmel kapcsolatos főbb fogalmak áttekintése. Ebből a szempontból a GDPR viszonylag kevés újdonságot hozott, hiszen a legfontosabb definíciókat már a 95/46/EK számú adatvédelmi irányelv is tartalmazta. A rendelet tulajdonképpen ezeket a fogalmakat vette át, néhány helyen kiegészítve, pontosítva azokat.

Az adatvédelmi jog legfontosabb alapfogalma kétségkívül a személyes adat. A rendelet – az irányelvhez hasonlóan – egy meglehetősen lényegre törő definíciót alkalmaz, mely szerint személyes adatnak minősül az azonosított vagy azonosítható természetes személyre (érintettre) vonatkozó bármely információ. Ez a fogalommeghatározás eléggé tágan értelmezi a személyes adatok körét, hiszen már a természetes személy közvetlen vagy közvetett azonosíthatósága is elegendő ahhoz, hogy személyes adatról beszéljünk. A személyes adatok legismertebb példái a természetes személyazonosító adatok (név, születési adatok, anyja neve), de szintén személyes adatnak tekinthetők az érintett testi, fiziológiai, genetikai, szellemi, gazdasági, kulturális vagy szociális azonosságára vonatkozó információk, valamint az érintettről készült kép- vagy hangfelvétel is.[52] A különösen érzékeny adatok kapcsán a GDPR egy-két új elem (pl. genetikai és biometrikus adatok) nevesítésén kívül csupán annyi változást hozott, hogy főszabályként megtiltotta a különösen érzékeny adatok kezelését, ami alól csak bizonyos feltételek esetén (pl. érintett hozzájárulása, egyén létfontosságú érdekeinek védelme, jelentős közérdek) ad kivételt.

A GDPR – az Infotv.-vel ellentétben – az adatkezelés és az adatfeldolgozás fogalma között nem tesz különbséget, mindössze az adatkezelésre ad egy általános definíciót. Ennek értelmében az adatkezelés magában foglal minden olyan tevékenységet, amely során személyes adatokon automatizált vagy nem automatizált módon valamilyen műveletet (pl. rögzítés, tárolás, lekérdezés, törlés) végeznek.[53] Ez a definíció lényegében megegyezik az Infotv. és az irányelv által használt fogalommal.

Míg korábban az Infotv. az adatkezelő és az adatfeldolgozó személyét a tevékenységük jellege alapján határolta el egymástól, addig a rendelet új megközelítést alkalmaz e téren. A GDPR rendelkezései szerint ugyanis a két funkció megkülönböztetésének fő szempontja az adatkezelési tevékenység céljának és eszközeinek meghatározása:[54]

---

[52] PÉTERFALVI – RÉVÉSZ – BUZÁS (2018), 64.
[53] Érdekesség, hogy bár a rendelet és az irányelv angol nyelvű verziója is a „processing" kifejezést használja, azonban a magyar nyelvű rendeletben ezt adatkezelésként, míg az irányelvben adatfeldolgozásként fordították.
[54] JÓRI – SOÓS – BÁRTFAI – HÁRI (2018), 92.

Adatkezelő	Adatfeldolgozó
Az adatkezelő lehet természetes vagy jogi személy, közhatalmi szerv, ügynökség vagy bármely egyéb szerv.	Az adatkezelőtől elkülönült személy vagy szervezet (pl. kiszervezett tevékenységet végzők).
Az adatkezelő határozza meg (önállóan vagy másokkal együtt) a személyes adatok kezelésének céljait és eszközeit.	Az adatfeldolgozó a célt és az eszközt nem határozhatja meg (ha mégis megteszi, akkor ő maga is adatkezelőnek minősül).
Az adatkezelő mindig a saját nevében jár el.	Az adatfeldolgozó az adatkezelő nevében jár el, a két fél közötti adatfeldolgozói szerződés alapján.
Az adatkezelő a saját döntései szerint jár el.	Az adatfeldolgozó az adatkezelő utasításai szerint jár el.
Az adatkezelő nem feltétlenül fér hozzá a kezelt adatokhoz.	Az adatfeldolgozónak mindig a birtokába kerül a személyes adat.
Az adatkezelés jogszerűségének elsőszámú felelőse, köteles a GDPR-nak való folyamatos megfelelést biztosítani, dokumentálni és szükség esetén igazolni.	

2. táblázat: Az adatkezelő és adatfeldolgozó közötti legfőbb különbségek

3.2.3. Az adatvédelem alapelvei

A korábbi szabályozáshoz hasonlóan a rendelet is külön fejezetet szentel az adatvédelmi alapelvek rögzítésének (GPDR 5. cikk). Ezek az elvek meghatározzák a személyes adatok védelmének általános keretrendszerét és elősegítik az érintettek jogérvényesítését.[55] A GDPR által definiált alapelveket az alábbi táblázatban foglaltam össze:

Alapelv	Magyarázat	Infotv.	Irányelv	Rendelet
Jogszerűség, tisztességes eljárás és átláthatóság	jogszabályi előírásoknak megfelelő adatkezelés, az érintett előzetes és teljes körű tájékoztatása mellett	✓	✓	✓
Célhoz kötöttség	adatkezelés csak meghatározott, egyértelmű és jogszerű céllal történhet	✓	✓	✓
Adattakarékosság	adatok csak a cél eléréséhez szükséges mértékben és ideig kezelhetők	✓	✓	✓
Pontosság	pontos és naprakész adatok követelménye	✓	✓	✓
Korlátozott tárolhatóság	adatok tárolása oly módon, amely az érintett azonosíthatóságát csak az adatkezelés céljához szükséges ideig teszi lehetővé	✓	✓	✓
Integritás és bizalmas jelleg	megfelelő technikai vagy szervezési intézkedések alkalmazása a személyes adatok biztonsága érdekében	✗	✗	✓
Elszámoltathatóság	az adatkezelő felelős az alapelvek betartásáért, és képesnek kell lennie ennek igazolására is	✗	✗	✓

3. táblázat: Az adatvédelem alapelvei

[55] PÉTERFALVI – RÉVÉSZ – BUZÁS (2018), 95.

Amint a fenti táblázatból is megállapítható, a rendeletben foglalt alapelvek többsége már az irányelvben és az Infotv.-ben is megjelent. A jogalkotó ugyanakkor két új alapelvet is bevezetett: az integritás és bizalmas jelleg elvét, illetve az elszámoltathatóság elvét. Az integritás és bizalmas jelleg elvének középpontjában az adatbiztonság követelménye áll. Az adatkezelő ugyanis köteles a megfelelő biztonsági intézkedéseket megtenni annak érdekében, hogy az adatokhoz való jogosulatlan hozzáférést és az adatok károsodását, elvesztését megakadályozza. Az adatbiztonság kritériumának alapelvként történő rögzítését az informatikai biztonság növekvő jelentősége tette szükségessé, amely a technológiai fejlődés következtében egyre komolyabb kihívás elé állítja az adatkezelőket.[56]

Az elszámoltathatóság elve nem csupán azt jelenti, hogy az adatkezelő felelős a rendeletben foglaltak betartásáért, hanem azt is, hogy szükség esetén ezt tudnia is kell igazolni az érintettek és az illetékes hatóságok felé. A gyakorlatban ez egy meglehetősen komoly adminisztratív terhet ró az adatkezelőkre, amely magában foglalja a megfelelő tájékoztató anyagok elkészítését, a belső adatvédelmi szabályzatok, eljárásrendek kialakítását és ezek megismerhetőségének biztosítását is. Hatósági vizsgálat esetén az adatkezelő többek között ezekkel a dokumentumokkal tudja bizonyítani, hogy megfelel a GDPR előírásainak.

3.2.4. Az adatkezelés jogalapjai

A jogszerűség elvének teljesítéséhez az adatkezelésnek minden esetben megfelelő jogalapra kell támaszkodnia. Míg a magyar adatvédelmi jog alapesetben csak az érintett hozzájárulása vagy törvény általi elrendelés esetén tette lehetővé személyes adatok kezelését, addig a GDPR – az irányelvre építve – jóval több jogalapot különböztet meg:[57]

[56] PÉTERFALVI – RÉVÉSZ – BUZÁS (2018), 107.
[57] JÓRI – SOÓS – BÁRTFAI – HÁRI (2018), 121-122.

3. ábra: Az adatkezelés GDPR szerinti jogalapjai

A személyes adatok kezelése akkor jogszerű, ha a fenti jogalapok közül legalább egy teljesül. Megfelelő jogalap hiányában az adatkezelés nem kezdhető el, a jogalap megszűnése esetén pedig azonnal meg kell szüntetni az adatok kezelését. Ha az adatkezelés egyidejűleg több jogalap alapján is lehetséges, akkor az adatkezelőnek választania kell közülük, ugyanis nem lehet az adatokat azonos célból több jogalapon is kezelni. A megfelelő jogalap kiválasztása azért is fontos, mert a különböző jogalapokhoz más-más érintetti jogok kapcsolódnak.[58]

Az Infotv. az adatkezelések elsődleges jogalapjának az érintett hozzájárulását, illetve a törvény általi elrendelést tekintette, ugyanakkor megkülönböztetett ún. másodlagos jogalapokat is (jogi kötelezettség teljesítése, jogos érdek érvényesítése, szerződés végrehajtása). Utóbbiak esetében azonban csak akkor lehetett személyes adatokat kezelni, ha az érintett hozzájárulásának megszerzése lehetetlen vagy aránytalanul nagy költséggel járt volna. Az Infotv.-ben nevesített jogalapok tulajdonképpen a GDPR-ban is megjelennek, azonban a rendelet valamennyi jogalapot egyenrangúnak tekinti, nem állít fel közöttük sorrendet.

A gyakorlatban az adatkezelés az esetek többségében az érintett hozzájárulásával történik.[59] A hozzájárulásra vonatkozó kritériumokat (önkéntesség, egyértelműség, megfelelő tájékoztatás) a 3.1. fejezetben, az Infotv. kapcsán korábban már bemutattam, a rendelet ehhez képest nem hozott számottevő változást. Az érintettek hozzájárulása mellett azonban gyakran

[58] KÉRI – KANCSAL (2018), 7.
[59] PÉTERFALVI – OSZTOPÁNI (2017), 392.

kerül sor adatkezelésre valamely szerződés teljesítéséhez kapcsolódóan is. Ebben az esetben a GDPR rendelkezései szerint két fontos kritériumnak kell teljesülnie: egyrészt az egyik szerződő félnek mindenképpen az érintettnek kell lennie, másrészt az adatkezelés és a szerződés célja között közvetlen és objektív kapcsolatnak kell fennállnia.[60] Ezek alapján például egy internetes vásárlás esetén a vevő nevének tárolása az adatkezelő részéről jogszerűnek tekinthető, hiszen az feltétlenül szükséges a szerződés teljesítéséhez.

Az adatkezelőre vonatkozó jogi kötelezettség teljesítése érdekében szintén kezelhetők személyes adatok. Ilyen, adatkezelésre feljogosító jogcímnek minősül például a bizonylatolási kötelezettség, illetve a pénzmosásra utaló pénzügyi tranzakciók kötelező bejelentése. Ezekkel kissé rokon kategória a közérdekű feladat ellátása és közhatalom gyakorlása érdekében végzett adatkezelés, amely lényegében megegyezik a magyar adatvédelmi jog által használt kötelező adatkezelés fogalmával.[61] Ide sorolható többek között a közhatalmi szervek adatkezelése, illetve az adóhatóság által feldolgozott adóbevallások is. A gyakorlatban az előző két jogalaphoz képest jóval ritkábban kerül sor személyes adatok kezelésére az érintett vagy egy másik természetes személy létfontosságú érdekeinek védelme miatt. Ezen jogalap alkalmazása a 29. cikk szerinti munkacsoport iránymutatása[62] alapján csak konkrét, közvetlen életveszéllyel járó esetekben (pl. járványok, természeti katasztrófák, stb.) lehetséges.

A fentieken kívül a rendelet lehetőséget nyújt arra is, hogy az adatkezelő a saját vagy egy harmadik fél jogos érdekében végezzen adatkezelést. Ez a jogalap egyfajta maradék kategóriának tekinthető, hiszen a gyakorlatban leginkább akkor szokták alkalmazni, amikor az előző öt jogalap egyike sem érvényesíthető az adott adatkezelési tevékenységre.[63] Jó példa az ilyen jogcímen végzett adatkezelésre a különböző kamerás megfigyelőrendszerek működtetése, illetve a banki hiteligénylések során bírálati céllal összegyűjtött adatok kezelése. Ebben az esetben a rendelet (47) preambulumbekezdésének megfelelően az adatkezelés megkezdése előtt ún. érdekmérlegelési tesztet kell végezni. Ennek során az adatkezelőnek bizonyítania kell, hogy valóban jogos érdeke fűződik az adatkezeléshez, és hogy az nem ütközik az érintett saját érdekeivel, jogaival. Az érdekmérlegelési teszt eredményéről az érintettet is tájékoztatni kell, aki tiltakozási jogával élve megtilthatja személyes adatainak kezelését.[64]

[60] PÉTERFALVI – RÉVÉSZ – BUZÁS (2018), 123.
[61] JÓRI – SOÓS – BÁRTFAI – HÁRI (2018), 156-160.
[62] 29. CIKK SZERINTI ADATVÉDELMI MUNKACSOPORT (2014), 21-22.
[63] PÉTERFALVI – RÉVÉSZ – BUZÁS (2018), 130.
[64] 29. CIKK SZERINTI ADATVÉDELMI MUNKACSOPORT (2014), 25-52.

3.2.5. *Az érintett jogai*

Dolgozatomban már említettem, hogy a személyes adatok védelmének középpontjában az információs önrendelkezési jog biztosítása áll. Ennek megfelelően az adatvédelmi szabályozás legfőbb célkitűzése egy olyan jogi keretrendszer megteremtése, mely lehetővé teszi az egyén számára, hogy saját maga rendelkezhessen a személyes adatairól. A GDPR bevezetése előtt az érintettek ezen joga sajnos csak korlátozottan érvényesült, éppen ezért a rendelet megalkotói kiemelt figyelmet fordítottak az érintetti jogok újra szabályozására annak érdekében, hogy az adatalany valódi kontrollt gyakorolhasson a személyes adatai felett.

A GDPR az érintettek jogainak vonatkozásában alapvetően a korábbi irányelvi szabályozásra épít, ugyanakkor számos helyen részletezi, kibővíti azt. A rendelet által nevesített érintetti jogokat a következő táblázatban foglaltam össze, ahol azt is feltüntettem, hogy az adott jog melyik alapelv érvényesülését biztosítja.

Átláthatóság elvét érvényre juttató jogok	Pontosság elvét érvényre juttató jogok	Egyéb érintetti jogok
• Tájékoztatáshoz való jog • Hozzáféréshez való jog • Adathordozhatósághoz való jog	• Helyesbítéshez való jog • Törléshez (elfeledtetéshez) való jog • Adatkezelés korlátozásához való jog	• Tiltakozáshoz való jog • Automatizált döntéshozatal esetén érvényesülő jogok

4. táblázat: Az érintett jogai

Forrás: PÉTERFALVI – RÉVÉSZ – BUZÁS (2018), 149-202. o. alapján saját készítés

3.2.5.1. Átláthatóság elvét érvényre juttató jogok

Az adatkezelés átláthatóságának követelménye talán a legfontosabb adatvédelmi alapelv az érintettek számára. Ezen kritériumnak megfelelően az adatalanyokat már az adatkezelés megkezdésekor tájékoztatni kell az adatkezelés céljáról, körülményeiről. Az érintett tájékoztatása az adatkezelő alapvető kötelezettsége, amelyet – az érintett többi jogosultságával ellentétben – az érintett ez irányú kérelme nélkül is kötelező teljesítenie.[65] A rendelet 13-14. cikke részletesen szabályozza a tájékoztató kötelező tartalmi elemeit, melyek közül az alábbiak a legfontosabbak:

– adatkezelő adatai, elérhetősége,

[65] European Union Agency for Fundamental Rights (2018), 207.

- adatkezelés célja, jogalapja,
- kezelt személyes adatok köre,
- személyes adatok címzettjei,
- adattárolás időtartama,
- érintett jogai, jogorvoslati lehetőségei.

A tájékoztatásnak főszabály szerint írásos formában kell történnie (beleértve a hagyományos papír alapú, illetve az elektronikus formátumot is), de az adatalany természetesen kérheti a szóbeli tájékoztatást is. Emellett – az átláthatóság elvének megfelelően – alapvető elvárás a tömör, könnyen érthető, közérthető nyelvezetű, könnyen és ingyenes hozzáférhető tájékoztató kialakítása. Az átláthatóság elve ezenkívül azt is megköveteli, hogy a tájékoztatásra a kellő időben, vagyis lehetőleg még az adatkezelési folyamat megkezdése előtt kerüljön sor.

A hozzáféréshez való jog szorosan kapcsolódik a tájékoztatáshoz való joghoz, hiszen ezen jogával élve az érintett ugyanúgy a személyes adatainak kezelésével összefüggésben kaphat tájékoztatást. Lényeges különbség azonban, hogy a hozzáférési jog keretében nemcsak az adatkezelés megkezdése előtt, hanem az adatkezelési tevékenység során bármikor, külön indoklás nélkül visszajelzést kérhet az érintett az adatkezelés részleteiről. A hozzáféréshez való jog gyakorlásához tehát minden esetben az érintett ez irányú kérelmére van szükség, amelyet az adatkezelőnek alapesetben 30 napon belül teljesítenie kell.

Az érintetti jogok kapcsán a GDPR egyik legfőbb újdonsága az adathordozhatósághoz való jog fogalmának bevezetése, amely tulajdonképpen a hozzáférési jog kiegészítésének tekinthető.[66] Ez alapján az érintett egyrészt jogosult arra, hogy az adatkezelő rendelkezésére bocsátott személyes adatait jól strukturált formátumban megkapja, másrészt pedig kérheti ezen adatok más adatkezelőhöz történő, közvetlen továbbítását is. Az adathordozhatósághoz való jog ugyanakkor csak az érintett hozzájárulásán vagy szerződésen alapuló jogcímek esetén, és kizárólag gépi, automatizált adatkezelések vonatkozásában gyakorolható.

3.2.5.2. Pontosság elvét érvényre juttató jogok

Az érintetti jogok következő csoportjába azok a jogosultságok tartoznak, amelyek a pontosság elvének gyakorlatban történő érvényesülését segítik elő. A rendelet három ilyen jellegű jogot nevesít: (1) a helyesbítéshez, (2) a törléshez (elfeledtetéshez), illetve (3) az adatkezelés korlátozásához való jogot. Az érintett a helyesbítési jogával élve a rá vonatkozó

[66] PÉTERFALVI – RÉVÉSZ – BUZÁS (2018), 171. o.

pontatlan személyes adatok javítását és a hiányos adatok kiegészítését kérheti. Az adatok helyesbítését az adatkezelőnek indokolatlan késedelem nélkül, a lehető leghamarabb el kell végeznie.

Az adatkezelés kapcsán a törléshez való jog az érintett egyik legerősebb jogosítványa.[67] Bár az adattakarékosság elvének értelmében a személyes adatokat csak az adatkezelés céljának elérését követően kell kötelezően törölni, a rendelet azonban jogosultságot biztosít az érintett számára, hogy már a cél megvalósulása előtt is kérhesse a személyes adatai törlését. Érdekes módon a jogalkotó az érintett törlési jogát kissé összemossa az adatkezelő törlési kötelezettségével, pedig a két fogalom nem ekvivalens egymással. Az adatkezelőnek ugyanis bizonyos esetekben nemcsak az érintett kérelmére, hanem egyéb okok (pl. jogszabályi előírások) miatt is törlési kötelezettsége keletkezhet. A rendelet ennek ellenére mind az érintett törlési jogát, mind az adatkezelő törlési kötelezettségét egy helyen, a 17. cikkben szabályozza.

Az érintett a törlési jogát tulajdonképpen a hozzájárulásának visszavonásával vagy tiltakozási jogával élve gyakorolhatja, minden egyéb esetben az adatkezelőnek az érintett kérelme nélkül is a lehető leghamarabb törölnie kell a személyes adatokat.[68] A törléshez, elfeledtetéshez való jog egy speciális esetének tekinthető emellett az is, hogy az érintettek kérhetik a nevüket tartalmazó keresési találatok eltávolítását az online keresőmotorok (pl. Google) találati listájáról, valamint kezdeményezhetik az interneten közzétett személyes adataikra mutató linkek, honlapok törlését.

Nevével ellentétben a törlési jog gyakorlása nem feltétlenül vonja maga után a személyes adatok tényleges törlését, fizikai megsemmisítését. A törlés ugyanis az adatvédelmi jog szerint (lásd Infotv. 3. § 13. pont) a személyes adatok felismerhetetlenné tételét jelenti oly módon, hogy az érintett és személyes adatai közötti kapcsolat többé már ne legyen helyreállítható. Ez az adatok fizikai megsemmisítésén kívül álnevesítéssel (anonimizálással) is megvalósítható, aminek következtében többé már nem lehet megállapítani, hogy az adott információ melyik érintettre vonatkozik, így az információ elveszti személyes adat jellegét.[69]

A pontosság elvéhez kapcsolódó harmadik érintetti jog az adatkezelés korlátozásához való jogosultság. Az adatkezelés korlátozására átmeneti, bizonytalan adatkezelési helyzetek esetén (pl. az érintett vitatja a személyes adatok pontosságát, az érintett ellenzi a jogellenesen

[67] PÉTERFALVI – RÉVÉSZ – BUZÁS (2018), 180.
[68] JÓRI – SOÓS – BÁRTFAI – HÁRI (2018), 286.
[69] PÉTERFALVI – RÉVÉSZ – BUZÁS (2018), 186.

kezelt adatok törlését, stb.) lehet szükség.[70] Az érintett ilyen esetekben kérelmezheti az adatkezelés ideiglenes szüneteltetését, felfüggesztését.

3.2.5.3. Egyéb érintetti jogok

A GDPR a fentieken kívül még egyéb, konkrét adatvédelmi alapelvhez nem köthető érintetti jogokat is nevesít: a tiltakozáshoz való jogot, illetve az automatizált döntéshozatal esetén érvényesülő jogot. A tiltakozáshoz való jogot a törlési és a korlátozási jog kapcsán egy kissé már érintettük, hiszen az érintett tiltakozásának egyik jogkövetkezménye éppen az adatok törlése vagy az adatkezelés korlátozása lehet. Fontos ugyanakkor kiemelni, hogy a tiltakozási jog kizárólag a jogos érdeken alapuló, illetve a közérdekű célból végzett adatkezelések esetén illeti meg az érintettet. Az érintett tiltakozása esetén az adatkezelő csak abban az esetben kezelheti tovább a személyes adatokat, ha bizonyítani tudja, hogy az adatkezelést olyan, kényszerítő erejű jogos okok indokolják, amelyek elsőbbséget élveznek az érintett érdekeivel szemben, vagy amelyek jogi igények érvényesítéséhez, védelméhez kapcsolódnak.

Az utolsó érintetti jog, az automatizált adatkezeléssel hozott döntés alóli mentesülés a modern kor technológiai vívmányaira adott válaszként is értelmezhető. Napjainkban ugyanis egyre gyakrabban fordul elő az, hogy személyes adatokat felhasználva, automatizált módon, emberi beavatkozás nélkül hoznak döntéseket az érintettel kapcsolatban. Jó példa erre a benyújtott hitelkérelmek automatizált elbírálása, vagy az emberi közreműködés nélkül hozott döntés az egyetemi felvételizőkről. Mivel ezek az adatkezelések jelentősen befolyásolhatják az egyén életkörülményeit, ezért az érintett jogosult arra, hogy mentesüljön a teljesen automatizált adatkezelésen alapuló döntések hatálya alól. Az érintett ezen jogkörével azonban csak akkor élhet, ha a döntést teljes mértékben automatizált módon, emberi beavatkozás nélkül hozták meg, és az az érintettre nézve joghatással járna, vagy jelentős mértékben érintené őt. További korlátozás, hogy ezen mentesülési jog nem érvényesíthető, ha a döntés a felek közötti szerződés teljesítéséhez szükséges, ha a döntés meghozatalát jogszabály teszi lehetővé, vagy ha az érintett kifejezett hozzájárulását adta az automatizált döntéshozatalhoz.

[70] JÓRI – SOÓS – BÁRTFAI – HÁRI (2018), 287.

3.2.6. Az adatkezelő és adatfeldolgozó kötelezettségei

Az előző fejezetekben már betekintést nyerhettünk abba, hogy a GDPR előírásainak való megfelelés a gyakorlatban mekkora többletterhet ró az adatkezelőkre és az adatfeldolgozókra. Az adatkezelők kötelezettségei elsősorban az érintetti jogok biztosításához (pl. tájékoztatási kötelezettség, hozzáférés) kapcsolódnak, mindazonáltal a rendelet még további feladatokat is előír az adatkezelők számára. Ezen feladatok ellátása során az adatkezelőnek tekintettel kell lennie a beépített és alapértelmezett adatvédelem 25. cikkben rögzített elvére, mely szerint az adatvédelmi megfontolásokat már az adatkezelés megkezdése előtt figyelembe kell venni, és az adatkezelés teljes folyamatában érvényesíteni kell azokat.

A GDPR értelmében az adatkezelési tevékenység jogszerűségének elsőszámú felelőse az adatkezelő, aki az elszámoltathatóság alapelvével összhangban köteles a rendeletnek való folyamatos megfelelést biztosítani, illetve ezt megfelelő dokumentumokkal alátámasztani. Ennek legfőbb eszköze a belső adatvédelmi nyilvántartások, szabályzatok és eljárásrendek kialakítása. Az adatkezelőnek az általa végzett adatkezelési tevékenységekről részletes és teljes körű nyilvántartást kell vezetnie, melynek alapvetően ugyanazokat az információkat kell tartalmaznia, mint az érintetti tájékoztatónak. A nyilvántartási kötelezettség kiterjed az adatfeldolgozók által az adatkezelők nevében végzett adatkezelési tevékenységekre is.

Érdemes megemlíteni, hogy a fent bemutatott nyilvántartási kötelezettség már az irányelvben (illetve ennek nyomán az Infotv.-ben) is megjelent. Ugyanakkor lényeges különbség, hogy ezen nyilvántartásokat korábban az illetékes felügyeleti hatóság (pl. NAIH) vezette. Az adatkezelőnek ugyanis az adatkezelési tevékenység megkezdése előtt értesítenie kellett a felügyeleti hatóságot az általa végzett, személyes adatokra vonatkozó adatkezelésekről. Ezt az általános jellegű bejelentési kötelezettséget azonban a GDPR megszüntette, és az adatvédelmi nyilvántartások vezetését egyértelműen az adatkezelő felelősségi körébe sorolta.[71]

Az adatkezelők egy másik fontos kötelezettsége az adatok biztonságának garantálása. Az GDPR 32. cikke ennek kapcsán csak általános elvárásokat fogalmaz meg, mely szerint az adatkezelőnek és az adatfeldolgozónak kötelessége megtenni a szükséges technikai és szervezési intézkedéseket annak érdekében, hogy az adatkezelés kockázatának megfelelő szintű adatbiztonságot garantálni tudják. A jogalkotó által használt általános megfogalmazás előnye, hogy az adatkezelő az adatbiztonsági intézkedések konkrét formáját az elérhető technológiai megoldások, azok költsége, illetve az adatkezelés jellege alapján határozhatja meg.

[71] PÉTERFALVI – RÉVÉSZ – BUZÁS (2018), 208-209.

Az adatkezelő fent bemutatott kötelezettségei alapvetően a személyes adatokkal való visszaélések megelőzését szolgálják. A GDPR ezenkívül azonban kiemelt figyelmet fordít arra is, hogy az adatvédelmi követelmények megsértése (vagyis az ún. adatvédelmi incidensek) esetén milyen intézkedéseket kell tennie az adatkezelőnek. A rendelet 4. cikkének 12. pontja értelmében adatvédelmi incidensnek tekinthető a biztonság minden olyan sérülése, amely a kezelt személyes adatok véletlen vagy jogellenes megsemmisítéséhez, megváltoztatásához vagy az adatokhoz való jogosulatlan hozzáféréshez vezet. A rendelet előírásai szerint a bekövetkező adatvédelmi incidenseket az adatkezelő az észlelést követően, 72 órán belül köteles bejelenteni a felügyeleti hatóságnak[72]. A bejelentés során az incidens összes lényeges körülményét ismertetni kell, beleértve az adatvédelmi incidens jellegét (pl. incidens típusa, érintettek kategóriái, az incidenssel érintett adatok köre), az incidens várható következményeit, illetve az incidens orvoslására tett vagy tervezett intézkedéseket. A rendelet értelmében az adatkezelőnek belső nyilvántartást is kell vezetnie az általa feltárt adatvédelmi incidensekről, amely egyúttal lehetővé teszi a felügyeleti hatóság számára, hogy nyomon tudja követni az adatkezelő intézkedéseit az incidens orvoslása érdekében. Az érintettre nézve magas kockázattal járó incidensekről magát az érintettet is haladéktalanul tájékoztatni kell.

Az adatkezelő egyik újonnan előírt kötelezettsége az adatvédelmi hatásvizsgálat lefolytatása. Ennek célja, hogy az adatkezelő még az adatkezelést megelőzően felmérje a tervezett adatkezelés jellegét (pl. cél, jogalap, stb.), megvizsgálja az adatkezelési műveletek szükségességét és arányosságát, feltárja a személyes adatok kezeléséből származó esetleges kockázatokat, illetve bemutassa az ezen kockázatok kezelését célzó intézkedéseket. Az adatvédelmi hatásvizsgálat elvégzésére azonban csak abban az esetben van szükség, ha az adatkezelés valószínűsíthetően magas kockázattal jár a természetes személyek jogaira és szabadságaira nézve. A rendelet ilyen, kifejezetten magas kockázattal járó adatkezelésnek tekinti (1) az automatizált adatkezelésen alapuló, értékelési vagy pontozási rendszerre épülő, az érintettre nézve joghatással bíró döntéshozatalt, (2) a különleges adatok nyilvántartását, (3) a bűncselekményekre vonatkozó személyes adatok nagy számban történő kezelését, valamint (4) a nyilvános helyek nagymértékű, módszeres megfigyelését.

Az előzőeken kívül a rendelet értelmében az adatkezelőknek és adatfeldolgozóknak bizonyos feltételek teljesülése esetén kötelességük adatvédelmi tisztviselőt kinevezni. Az adatvédelmi tisztviselő elsődleges feladata, hogy szakmai rátermettsége, hozzáértése révén

[72] Magyarországon az adatvédelmi incidensek bejelentését az adatkezelők a NAIH által külön erre a célra üzemeltetett Adatvédelmi Incidensbejelentő Rendszeren keresztül tehetik meg.

biztosítsa és elősegítse az adott szervezeten belül az adatvédelmi jogszabályoknak való megfelelést. Ennek során egyrészt felméri, ellenőrzi és véleményezi az adott szervezet meglévő adatkezelési tevékenységeit a jogszabályi elvárások fényében, másrészt hatékonyan közreműködik a tényleges adatkezelést megelőző adatvédelmi hatásvizsgálatok elvégzésében.

3.2.7. A felügyeleti hatóságokra vonatkozó rendelkezések

A GDPR nemcsak az érintettek és az adatkezelők vonatkozásában határoz meg jogszabályi előírásokat, hanem a felügyeleti hatóságok működésére is jelentős hatást gyakorolt. A tagállami szintű felügyeleti hatóságok[73] felállításáról már az adatvédelmi irányelv is rendelkezett, ugyanakkor az irányelvi szabályozás eltérő implementálásából adódóan az egyes hatóságok jogértelmezése sok esetben különbözött egymástól. A közvetlenül alkalmazandó általános adatvédelmi rendelet azonban számottevően csökkentette az egyes tagállamok felügyeleti hatóságainak mozgásterét, egységesítve ezzel az adatvédelmi szabályok alkalmazását és ellenőrzését az egész Európai Unióban.

A rendelet általános jelleggel szabályozza a nemzeti felügyeleti hatóságok jogállását, feladat- és hatáskörüket, valamint a hatóságok közötti együttműködés keretrendszerét. Jogállását tekintve a felügyeleti hatóság független közhatalmi szerv, amelynek elsődleges célja a természetes személyek alapvető jogainak védelme a személyes adataik kezelése tekintetében. A rendelet 58. cikke a felügyeleti hatóságok feladatait három hatáskör mentén csoportosítja: (1) vizsgálati hatáskör, (2) korrekciós hatáskör, illetve (3) engedélyezési és tanácsadási hatáskör. A felügyeleti hatóság vizsgálati hatáskörében eljárva adatvédelmi auditokat folytat, és ellenőrzi az adatkezelő tevékenységének jogszabályi megfelelőségét. Az adatvédelmi előírások megsértése esetén a hatóság korrekciós jogkörével élve figyelmezteti az adatkezelőt, elrendelheti az adatkezelés korlátozását, illetve közigazgatási bírság kiszabásáról is dönthet. Végül a hatóság feladatai közé tartozik a személyes adatok kezelésével kapcsolatos engedélyek, tanúsítványok kiadása, valamint a jogalkotó és az adatkezelők számára történő tanácsadás is.

A GDPR jogalkotói – felismerve a határon átnyúló adatkezelések növekvő szerepét napjaink globalizált világában – külön fejezetet szenteltek a felügyeleti hatóságok közötti együttműködés szabályozására, elősegítésére. A rendelet értelmében a határokon átnyúló ügyekben az adatvédelmi hatóságoknak együtt, közösen kell fellépniük. Az ún. egyablakos

[73] Hazánkban a felügyeleti hatóság szerepét a Nemzeti Adatvédelmi és Információszabadság Hatóság (NAIH) tölti be, melynek jogállását az Infotv. szabályozza.

ügyintézés (*one-stop shop*) érdekében ilyen esetben ki kell jelölni a fő felügyeleti hatóságot, akivel az adatkezelő az eljárás során tarthatja a kapcsolatot. Főszabály szerint ezt a szerepet az adatkezelő tevékenységi központja szerint illetékes adatvédelmi hatóság tölti be. A fő felügyeleti hatóság koordinálja az együttműködést a többi érintett hatósággal, akik a releváns információk megosztásán és a segítségnyújtáson kívül véleményezhetik a fő felügyeleti hatóság által készített döntéstervezetet is.

A személyes adatok védelméhez való jog és a GPDR-ban foglalt rendelkezések érvényesülésének ellenőrzésében a nemzeti felügyeleti hatóságok mellett fontos szerepet játszik az Európai Adatvédelmi Testület is. Ez a jogi személyiséggel rendelkező uniós szerv az egyes tagállamok felügyeleti hatóságainak vezetőiből és az európai adatvédelmi biztosból áll. A Testületet az irányelv 29. cikke szerinti adatvédelmi munkacsoport jogutódjaként hozták létre abból a célból, hogy általános iránymutatásaival, ajánlásaival segítse az adatvédelmi szabályok Unión belüli egységes alkalmazását, értelmezését.[74]

3.2.8. Jogorvoslat, szankciók

Az érintettek a személyes adataik kezelése kapcsán tapasztalt jogsértések orvoslása érdekében elsősorban az illetékes felügyeleti hatósághoz fordulhatnak. Ahogy azt korábban már említettem, az adatvédelmi hatóság – mérlegelve a jogsértés természetét és súlyosságát – korrekciós hatáskörében eljárva számos szankciót alkalmazhat az adatkezelőkkel vagy adatfeldolgozókkal szemben. Ezek közül kétségkívül a kiszabható közigazgatási bírság mértéke váltotta ki a legnagyobb visszhangot a közvélemény körében, amely egyúttal a GDPR egyik legfontosabb újdonságának tekinthető. A rendelet ugyanis az irányelvvel ellentétben rögzítette a kiszabható közigazgatási bírság maximális mértékét: a felügyeleti hatóság különösen súlyos jogsértések esetén (pl. alapelvek vagy érintetti jogok megsértése, jogszerűtlen adatkezelés, hatósági utasítás be nem tartása) akár 20 millió EUR vagy az adatkezelő előző évi világpiaci forgalmának 4%-át kitevő összegű bírságot is kivethet (a kettő közül a magasabb alkalmazandó).[75] Mindez tehát a NAIH által korábban kivethető 20 millió Ft-os bírságnál nagyságrendekkel súlyosabb büntetést jelenthet az adatkezelők számára.

[74] European Union Agency for Fundamental Rights (2018), 199-200.
[75] A kevésbé súlyos jogsértések (pl. gyermekekre vonatkozó szabályok megsértése, adatkezelői kötelezettségek elmulasztása) esetén a maximális bírság 10 millió EUR vagy az adatkezelő előző évi világpiaci forgalmának 2%-a (a kettő közül a magasabb).

A GDPR a fentieken kívül lehetőséget biztosít a bírósági jogorvoslatra is. Amennyiben az adatkezelés nem felel meg a rendelet előírásainak, akkor az érintettek közigazgatási pert indíthatnak az adatkezelővel vagy adatfeldolgozóval szemben. Ha az érintett panasza jogos, és a jogsértés az érintett számára vagyoni vagy nem vagyoni kárt okozott, akkor a bíróság az adatkezelő vagy az adatfeldolgozó számára kártérítési kötelezettséget írhat elő. Bírósági eljárás az adatkezelőn kívül a felügyeleti hatósággal szemben is kezdeményezhető: mind az érintett, mind az adatkezelő kifogást emelhet a bíróságon a hatóság döntése ellen.

4. A GDPR EDDIGI GYAKORLATI TAPASZTALATAI

Bár az általános adatvédelmi rendelet bevezetése óta még csak közel egy év telt el, szakdolgozatom utolsó részében – az előző fejezetek elméleti jellegű elemzését követően – szeretném röviden összegezni az eddig eltelt időszak legfontosabb gyakorlati tapasztalatait. Ennek során elsősorban a hazai és a tagállami adatvédelmi hatóságok által közzétett elemzésekre támaszkodom, mivel a rendelet alkalmazásának körülményeiről leginkább a felügyeleti hatóságok rendelkeznek átfogó képpel. Ennek kapcsán személyes interjút készítettem a Nemzeti Adatvédelmi és Információszabadság Hatóság elnökével, Dr. Péterfalvi Attilával, amelyet szintén felhasználok a GDPR jelentette gyakorlati kihívások bemutatásához.

Az általános adatvédelmi rendelet 2016-os hatályba lépését követően a jogalkotó 2 év türelmi időszakot biztosított az adatkezelőknek és a felügyeleti hatóságoknak a rendeletben foglalt előírások teljesítésére. A felkészülés során az adatkezelőknek felül kellett vizsgálniuk az adatkezelési tevékenységük teljes folyamatát (pl. adatvagyon feltérképezése, belső adatvédelmi szabályzatok, tájékoztatók kialakítása, stb.), amely komoly anyagi, informatikai és adminisztratív terhet rótt az adatkezelőkre, különösen a kis- és középvállalkozásokra. Emiatt a kétéves türelmi időszak sokak számára nem bizonyult elegendőnek, amit a Cisco Systems által 2019 januárjában közzétett felmérés[76] is megerősít. A 3.206 vállalat bevonásával készített, globális szintű tanulmány szerint ugyanis a GDPR bevezetése után fél évvel az adatkezelők mindössze 59%-a gondolta azt, hogy teljes mértékben megfelel a rendelet előírásainak. A megkérdezettek 38%-a ezzel szemben a felmérés időpontjában még nem teljesítette maradéktalanul a GDPR követelményeit. Érdemes még megemlíteni, hogy a felmérésben részt vevő adatkezelők szerint az adatbiztonsági követelmények teljesítése, a munkavállalók

[76] Cisco Systems (2019)

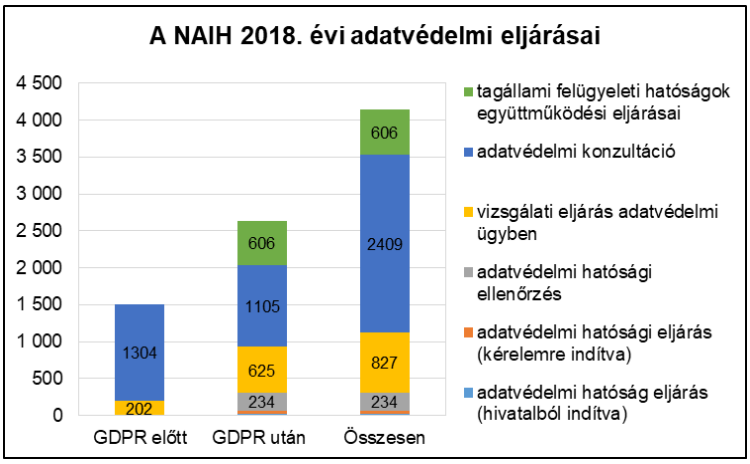
adatvédelmi képzése, valamint a változó jogszabályi környezetnek és a beépített adatvédelem elvének való megfelelés bizonyult a GDPR-ra való felkészülés legkritikusabb területeinek.

Az adatkezelők általános felkészültségét mérte fel az Európai Bizottság által az adatvédelem nemzetközi világnapja (január 28.) alkalmából készített tájékoztató[77] is, amely összesítette a nemzeti adatvédelmi hatóságok által nyilvántartott adatokat. Ez alapján a GDPR 2018. májusi bevezetése és 2019. január között mintegy 95 ezer adatvédelmi panasz érkezett az érintettektől a felügyeleti hatóságokhoz, melyek többsége a marketing célú (telefonos vagy e-mailes) megkeresésekre, illetve a kamerával történő megfigyelésekre vonatkozott. Az adatkezelők a vizsgált időszakban összesen 41.502 adatvédelmi incidenst jelentettek a hatóságok felé, amely tagállamonként átlagosan havi 185 darabnak felel meg.

A fenti ügyek közül súlyosságát tekintve egyértelműen kiemelkedik a Google esete, amelyre a francia adatvédelmi hatóság (CNIL) 2019 januárjában 50 millió eurós bírságot szabott ki a felhasználók nem megfelelő, hiányos tájékoztatása miatt. A hatóság közleménye[78] szerint a vállalat adatvédelmi tájékoztatója csak széttagoltan, egymástól 5-6 kattintásnyi távolságra lévő dokumentumokban volt csak elérhető. Ráadásul a cég azon megoldása, hogy a személyre szabott hirdetésekhez való hozzájárulás opciója alapértelmezetten be volt jelölve, nem felelt meg a GDPR azon követelményének, mely szerint az érintett hozzájárulásának konkrét, egyértelmű megerősítő cselekedettel kell történnie. A fentiek miatt kiszabott, meglehetősen súlyos bírságot a francia adatvédelmi hatóság egyrészt a jogsértés folyamatos, állandó jellegével, másrészt a hátrányosan érintett személyek jelentős számával indokolta.

Ami a hazai statisztikákat illeti, a NAIH 2018. évi beszámolója[79] részletes adatokat tartalmaz a hatóság adatvédelmi eljárásaival, ügyeivel kapcsolatban. A beszámoló alapján 2018-ban összesen 4.143 adatvédelmi eljárásra került sor, amely az előző évhez képest szignifikáns emelkedést jelent. Az eljárások kétharmadát a GDPR bevezetését követően indították meg, ami jól mutatja az adatvédelmi szabályok szigorodását. Az eljárások közül a konzultációs beadványok száma például az előző évihez képest közel duplájára nőtt, ami jelzi az új szabályozás körüli bizonytalanságot.[80]

[77] Európai Bizottság (2019)
[78] Commission Nationale de l'Informatique et des Libertés (2019)
[79] Nemzeti Adatvédelmi és Információszabadság Hatóság (2019)
[80] A beszámoló ugyanakkor kiemeli, hogy a GDPR értelmezésére – az egységes európai jogalkalmazás érdekében – elsősorban az Európai Adatvédelmi Testület jogosult, így a NAIH mozgástere ebből a szempontból korlátozott.



4. ábra: A NAIH 2018. évi adatvédelmi eljárásai[81]
Forrás: NAIH (2019), 6-9. alapján saját szerkesztés

A GDPR bevezetését követően a NAIH nyilvántartása szerint 50 hatósági eljárás iránti kérelmet nyújtottak be, melyek jellemzően a munkahelyi, egészségügyi és banki adatkezeléshez, az érintetti jogok (pl. hozzáférési jog) teljesítésének megtagadásához, illetve elmulasztásához, valamint a kamerás megfigyelésekhez kapcsolódtak.[82] A felügyeleti hatóság vizsgálati rendszerében a GDPR hatályba lépése után új elemként jelentek meg az adatvédelmi incidensek nyomán megindított hatósági ellenőrzések. Az adatkezelők 2018-ban összesen 244 db adatvédelmi incidenst jelentettek be a NAIH-hoz. Ez a meglehetősen alacsony, átlagosan napi 1,1 incidensnek megfelelő szám ugyanakkor arra utal, hogy a jogalanyok még nincsenek teljesen tisztában az adatvédelmi incidens fogalmával és azok kötelező bejelentésével. Az incidensek többsége a felügyelet statisztikái szerint az alábbi jogsértésekből fakadt:[83]

- téves címre küldött postai és elektronikus levelek,
- e-mail címek illetéktelen kezekbe jutása azáltal, hogy a címzettek a „Titkos másolat” mező helyett tévesen a „Másolatot kap” mezőben lettek felsorolva,
- az adatkezelőt ért hackertámadás következtében kiszivárgott személyes adatok,
- ellopott/elvesztett számítástechnikai eszközök, telefonok.

A NAIH honlapján közzétett hatósági határozatok alapján hazánkban a GDPR megsértéséért az első bírságot 2018. december 21-én vetette ki a hatóság, míg az eddigi legsúlyosabb bírság és egyben a legnagyobb sajtóvisszhangot kiváltó ügy a Demokratikus Koalíció párt jogsértéséhez kapcsolódott. A NAIH határozata[84] szerint a párt által üzemeltetett

[81] Mivel az Infotv. GDPR-nak megfelelő módosítására csak 2018. július 26-án került sor, ezért a NAIH csak ezt követően kezdte meg az új típusú, a rendelettel összhangban lévő adatvédelmi hatósági eljárások lefolytatását.
[82] Nemzeti Adatvédelmi és Információszabadság Hatóság (2019), 12-13.
[83] Nemzeti Adatvédelmi és Információszabadság Hatóság (2019), 77-78.
[84] NAIH/2019/2668/2 határozat (előzmény: NAIH/2018/5457/V)

honlapot hackertámadás érte, melynek következtében személyes adatok (e-mail címek, felhasználói nevek és jelszavak) kerültek ki az internetre nyilvánosan elérhető formában. A párt ennek kapcsán elmulasztotta az incidensbejelentési kötelezettségét, valamint az érintetteket sem tájékoztatta az esetről. A Demokratikus Koalícióra kiszabott, meglehetősen súlyos, 11 millió Ft-os bírságot a hatóság azzal indokolta, hogy az incidens kifejezetten magas kockázattal járt: egyrészt különlegesen érzékeny, politikai véleményre vonatkozó adatok szivárogtak ki, másrészt az eset viszonylag sok (több mint 6.000) felhasználót érintett.

A GDPR 2018-as bevezetése természetesen a NAIH szervezetében, működésében is jelentős változásokat hozott. Az új jogszabály következtében a hatóság feladatköre a korábbiakhoz képest kibővült, amit részben az intézményi struktúra átalakításával és új szervezeti egységek (pl. Engedélyezési és Incidensbejelentési Főosztály, GDPR-munkacsoport) létrehozásával oldottak meg.[85] Mindez természetesen a munkavállalók számának emelésével járt együtt: a létszám az előző évi 77 főről 114 főre emelkedett. Péterfalvi Attila elmondása szerint ezzel a NAIH adatvédelmi szakembereinek száma gyakorlatilag megduplázódott. A szervezet átalakítása azonban még korántsem fejeződött be, a jövőben még további létszámemelés várható.

A hatóság működése kapcsán Péterfalvi Attila emellett azt is kiemelte, hogy a rendelet bevezetésével szűkült a hatóság mozgástere az eljárások tekintetében: míg az Infotv. nagyobb választási lehetőséget biztosított az eljárás típusát illetően, addig a GDPR szigorúbban szabályozza a hatóság eljárási rendszerét. Ahogy azt az előzőekben már láthattuk, a GDPR hatályba lépése óta a hatósághoz beérkező panaszok száma is emelkedett, melynek eredményeképpen az egyes ügyek átfutási ideje is érezhetően megnőtt. Ennek következtében Péterfalvi Attila elmondása szerint a NAIH javaslatot tett az adatvédelmi hatóság eljárására rendelkezésre álló határidő 120 napról 150 napra történő emelésére.

[85] Nemzeti Adatvédelmi és Információszabadság Hatóság (2018b)

5. ÖSSZEFOGLALÁS

A 2018-as év egyik leggyakrabban emlegetett betűszava kétségkívül a GDPR volt. A nagy érdeklődést meglepő módon egy jogszabály, az Európai Unió által 2018-ban bevezetett általános adatvédelmi rendelet (angol nevén: *General Data Protection Regulation, GDPR*) váltotta ki, amely új alapokra helyezte a személyes adatok jogszabályi védelmét. Bár az adatvédelmi szabályozás már több évtizedes múltra tekint vissza, sokan csak a GDPR kapcsán szembesültek a személyes adatok védelmének fontosságával, kihívásaival. Szakdolgozatomban ezért elsősorban arra a kérdésre kerestem a választ, hogy a GDPR bevezetése milyen változásokat hozott az adatvédelmi szabályozásban.

Szakdolgozatom első részében a személyiségi jogok általános bemutatása mellett áttekintettem az európai és a hazai adatvédelmi szabályozás történetét. Az adatvédelmi jog a XX. század második felétől kezdődően a folyamatosan változó technológiai és társadalmi körülmények következtében gyors fejlődésen ment keresztül. A harmonizált, európai szintű adatvédelmi szabályozás alapjait az 1995-ben kiadott, 95/46/EK számú irányelv teremtette meg, amely a GDPR megalkotása előtt mintegy két évtizedig biztosította Európában a személyes adatok jogszabályi védelmét. Magyarországon az első, kimondottan az adatvédelemmel foglalkozó törvényt (Avtv.) 1992-ben alkotta meg az Országgyűlés, amelyet számos módosítás után 2011-ben az Infotv. váltott fel. Az Infotv. a GDPR mellett azóta is a hazai adatvédelmi szabályozás elsődleges jogforrásának számít.

A GDPR hatályba lépése előtti magyar szabályozás bemutatását követően, dolgozatom központi részében az általános adatvédelmi rendelet előírásait vettem tüzetesebb vizsgálat alá. A GDPR egyik legfontosabb újítása a korábbi szabályozáshoz képest, hogy a rendelet hatálya nemcsak az Európai Unión belüli, hanem azon Unión kívüli adatkezelésekre is kiterjed, ahol az adatkezelő tevékenységi hellyel rendelkezik az EU-ban, vagy az adatkezelés érintettje az Unióban tartózkodik. Az alapfogalmak, alapelvek kapcsán a rendelet elsősorban az irányelvben foglaltakra épít, ugyanakkor a jogalkotó két új alapelvet is bevezetett: egyrészt külön alapelvben rögzítette az adatbiztonság követelményét (integritás és bizalmas jelleg elve), másrészt az elszámoltathatóság elvének értelmében az adatkezelőnek szükség esetén tudnia kell igazolni a jogszabálynak való megfelelést.

Ezt követően rátértem az adatvédelem három központi szereplőjére (érintett, adatkezelő, felügyeleti hatóság) vonatkozó jogok és kötelezettségek ismertetésére. A GDPR az érintettek jogait illetően a korábbi irányelvi szabályozásra támaszkodik, ugyanakkor két új jogosultsággal

(elfeledtetéshez, illetve adathordozhatósághoz való jog) is felruházta őket. Az érintettekkel ellentétben a rendelet az adatkezelőkkel kapcsolatban már számos újdonságot hozott. Az adatkezelőknek például részletes és teljes körű belső nyilvántartást kell vezetniük az általuk végzett adatkezelési tevékenységekről, valamint adatvédelmi hatásvizsgálatot is kell végezniük a kifejezetten magas kockázattal járó adatkezelések előtt. Végül jelentős többletterhet ró az adatkezelőkre az is, hogy a jogszabályi követelmények megsértéséből fakadó adatvédelmi incidenseket 72 órán belül kötelezően be kell jelenteniük a hatóság részére.

A GDPR egyik legfőbb előnye, hogy a rendeleti formában történő szabályozásnak köszönhetően megszüntette a tagállami felügyeleti hatóságok helyenként eltérő jogi megközelítéseit. A rendelet emellett külön figyelmet fordított a felügyeleti hatóságok közötti nemzetközi együttműködés szabályozására is. További újdonságot jelent, hogy a jogszabályi rendelkezések megsértése esetén kiszabható maximális bírság mértéke jelentősen emelkedett: a hatóság a korábbi 20 millió Ft helyett akár 20 millió euró (azaz több mint 6 milliárd Ft), vagy az adott vállalkozás előző évi forgalmának 4%-át kitevő összegű bírságot is kivethet.

A GDPR általános jellegű bemutatását követően, dolgozatom utolsó részében a rendelet bevezetése óta eltelt időszak legfontosabb gyakorlati tapasztalatait foglaltam össze. Ennek során egy nemzetközi tanulmány alapján megmutattam, hogy az adatkezelők közel 40%-a a GDPR hatályba lépése után fél évvel még nem állt készen a rendelet előírásainak teljesítésére. Ezt követően hazai és uniós statisztikák segítségével elemeztem a hatósági eljárásokat, és részletesen ismertettem a legsúlyosabb bírságot kiváltó jogeseteket. Végezetül a Nemzeti Adatvédelmi és Információszabadság Hatóság (NAIH) elnökével, Dr. Péterfalvi Attilával készített személyes interjúm alapján összefoglaltam, hogy milyen hatást gyakorolt a NAIH működésére a GDPR bevezetése.

Szakdolgozatomat összegezve megállapítható, hogy bár az általános adatvédelmi rendelet erősen épít a korábbi szabályozásra, véleményem szerint a GDPR új mérföldkőnek tekinthető a személyes adatok védelmében. Ugyanakkor annak eldöntéséhez, hogy a rendelet valóban be fogja-e váltani a hozzá fűzött reményeket, sajnos még nem telt el elegendő idő. Az adatvédelmi szabályozás fejlődése ráadásul még korántsem ért véget. A közeljövőben várható például az európai adatvédelmi reformcsomag következő elemének, az ún. e-privacy rendeletnek a bevezetése, amely az elektronikus hírközlés keretében végzett adatkezelések speciális szabályait fogja tartalmazni. Emellett további kihívást jelenthet a személyes adatok védelmével kapcsolatos jogharmonizáció további folytatása és a GDPR rendelkezéseinek

Európán kívüli országokra (pl. USA) történő kiterjesztése is. Mindezek alapján tehát az adatvédelmi jog várhatóan a jövőben is az egyik legdinamikusabban fejlődő jogterület lesz.

IRODALOMJEGYZÉK

1. Cisco Systems (2019): *Maximizing the value of your data privacy investments – Data Privacy Benchmark Study*. Cisco Cybersecurity Series 2019, Data Privacy, 2019. január. https://www.cisco.com/c/dam/en_us/about/doing_business/trust-center/docs/dpbs-2019.pdf, Letöltés dátuma: 2019. március 29.
2. Commission Nationale de l'Informatique et des Libertés (2019): *The CNIL's restricted committee imposes a financial penalty of 50 Million euros against GOOGLE LLC*. https://www.cnil.fr/en/cnils-restricted-committee-imposes-financial-penalty-50-million-euros-against-google-llc, Letöltés dátuma: 2019. március 29.
3. Európai Bizottság (2019): *GDPR in numbers*.
4. https://ec.europa.eu/commission/sites/beta-political/files/190125_gdpr_infographics_v4.pdf, Letöltés dátuma: 2019. március 29.
5. European Data Protection Supervisor (2018): *The History of the General Data Protection Regulation*. https://edps.europa.eu/data-protection/data-protection/legislation/history-general-data-protection-regulation_en, Letöltés dátuma: 2019. január 6.
6. European Union Agency for Fundamental Rights (2018): *Handbook on European data protection law – 2018 edition*. Publications Office of the European Union, Luxembourg. https://fra.europa.eu/sites/default/files/fra_uploads/fra-coe-edps-2018-handbook-data-protection_en.pdf, Letöltés dátuma: 2019. március 7.
7. JAY, R. – HAMILTON, A. (1999): *Data Protection – Law and Practice*. Sweet & Maxwell, London.
8. JÓRI András (2005): *Adatvédelmi kézikönyv*. Osiris Kiadó, Budapest.
9. JÓRI András (2006): *A nyilvánosság határai: a személyes adat, a közérdekű adat és a közérdekből nyilvános adat fogalma az adatvédelmi biztos és az Alkotmánybíróság gyakorlatában*. In: PÉTERFALVI Attila szerk.: Tízéves az Adatvédelmi Biztos Irodája. Adatvédelmi Biztos Irodája, Budapest. 109-122.
10. JÓRI András (2009): *Az adatvédelmi jog generációi és egy második generációs szabályozás részletes elemzése*. Doktori (PhD) értekezés, Pécsi Tudományegyetem, Pécs.
11. JÓRI András – HEGEDŰS Bulcsú – KEREKES Zsuzsanna szerk. (2010): *Adatvédelem és információszabadság a gyakorlatban*. CompLex Kiadó, Budapest.

12. JÓRI András – SOÓS Andrea Klára (2016): *Adatvédelmi jog – Magyar és európai szabályozás*. HVG-ORAC Kiadó, Budapest.
13. JÓRI András szerk. – SOÓS Andrea Klára – BÁRTFAI Zsolt – HÁRI Anita (2018): *A GDPR magyarázata*. HVG-ORAC Kiadó, Budapest.
14. KÉRI Ádám – KANCSAL Tamás (2018): *Adatvédelem a gyakorlatban – Készüljön fel velünk a GDPR-ra!* HVG Kiadó, Budapest.
15. LENKOVICS Barnabás – SZÉKELY László (2001): *A személyi jog vázlata*. Eötvös József Könyvkiadó, Budapest.
16. MAJTÉNYI László (2003): *Az információs jogok*. In: HALMAI Gábor – TÓTH Gábor Attila szerk.: Emberi jogok. Osiris Kiadó, Budapest. 577-637.
17. Majtényi László (2006): *Az információs szabadságok – adatvédelem és a közérdekű adatok nyilvánossága*. CompLex Kiadó, Budapest.
18. MAYER-SCHÖNBERGER, V. (1997): *Generational Development of Data Protection in Europe*. In: AGRE, P. E. – ROTENBERG, M. szerk.: Technology and Privacy: The New Landscape. The MIT Press, Cambridge, Massachusetts. 219-241.
19. MÉSZÁROS János (2017): *Adatvédelem a XXI. században és az internet világában*. Doktori (PhD) értekezés, Szegedi Tudományegyetem, Szeged.
20. Nemzeti Adatvédelmi és Információszabadság Hatóság (2018a): *Adatvédelmi értelmező szótár*. https://www.naih.hu/adatvedelmi-szotar.html, Letöltés dátuma: 2018. október 10.
21. Nemzeti Adatvédelmi és Információszabadság Hatóság (2018b): *Nemzeti Adatvédelmi és Információszabadság Hatóság elnökének 20/2015. (11.30.) sz. utasítása a Nemzeti Adatvédelmi és Információszabadság Hatóság szervezetének és működésének általános szabályairól (módosításokkal egységes szerkezetben)*.
22. https://www.naih.hu/files/2_1_SZMSZ_egyseges_2018_09_15.pdf, Letöltés dátuma: 2019. április 2.
23. Nemzeti Adatvédelmi és Információszabadság Hatóság (2019): *A Nemzeti Adatvédelmi és Információszabadság Hatóság Beszámolója a 2018. évi tevékenységéről*. https://www.naih.hu/files/Beszamolo-2018-MR.PDF, Letöltés dátuma: 2019. április 2.
24. PÉTERFALVI Attila szerk. (2012): *Adatvédelem és információszabadság a mindennapokban*. HVG-ORAC Kiadó, Budapest.

25. PÉTERFALVI Attila – OSZTOPÁNI Krisztián (2017): *A személyes adatok magánjogi védelme a Nemzeti Adatvédelmi és Információszabadság Hatóság gyakorlatában*. In: GÖRÖG Márta – MENYHÁRD Attila – KOLTAY András szerk.: A személyiség és védelme – Az Alaptörvény VI. cikkelyének érvényesülése a magyar jogrendszeren belül. ELTE Állam- és Jogtudományi Kar, Budapest. 389-403.
26. PÉTERFALVI Attila – RÉVÉSZ Balázs – BUZÁS Péter szerk. (2018): *Magyarázat a GDPR-ról*. Wolters Kluwer Kft., Budapest.
27. SZIKLAY Júlia (2011): *Az információs jogok kialakulása, fejlődése és társadalmi hatása*. Doktori (PhD) értekezés, Pécsi Tudományegyetem, Pécs.
28. SZŐKE Gergely László (2013): *Az adatvédelem szabályozásának történeti áttekintése*. Infokommunikáció és Jog, 10. évf., 3. szám, 107-112.
29. SZŐKE Gergely László (2014): *Az európai adatvédelmi jog megújítása – Tendenciák és lehetőségek az önszabályozás területén*. Doktori (PhD) értekezés, Pécsi Tudományegyetem, Pécs.
30. VÉKÁS Lajos – GÁRDOS Péter szerk. (2014): *Kommentár a Polgári Törvénykönyvhöz - Kommentár a Polgári Törvénykönyvről szóló 2013. évi V. törvényhez*. Wolters Kluwer Kft., Budapest.

Jogszabályok:

- Magyarország Alaptörvénye (2011. április 25.)
- 1977. évi IV. törvény a Magyar Népköztársaság Polgári Törvénykönyvéről szóló 1959. évi IV. törvény módosításáról és egységes szövegéről
- 1989. évi XXXI. törvény az Alkotmány módosításáról
- 1992. évi LXIII. törvény a személyes adatok védelméről és a közérdekű adatok nyilvánosságáról
- 2011. évi CXII. törvény az információs önrendelkezési jogról és a közérdekű adatok nyilvánosságáról
- 2013. évi V. törvény a Polgári Törvénykönyvről
- 2018. évi XXXVIII. törvény az információs önrendelkezési jogról és az információszabadságról szóló 2011. évi CXII. törvénynek az Európai Unió adatvédelmi reformjával összefüggő módosításáról, valamint más kapcsolódó törvények módosításáról

- Az Európai Parlament és a Tanács 95/46/EK irányelve (1995. október 24.) a személyes adatok feldolgozása vonatkozásában az egyének védelméről és az ilyen adatok szabad áramlásáról
- Az Európai Parlament és a Tanács (EU) 2016/679 rendelete (2016. április 27.) a természetes személyeknek a személyes adatok kezelése tekintetében történő védelméről és az ilyen adatok szabad áramlásáról, valamint a 95/46/EK rendelet hatályon kívül helyezéséről (általános adatvédelmi rendelet)

Egyéb joganyagok:

- Egyesült Nemzetek Szervezete (1948): *Az Emberi Jogok Egyetemes Nyilatkozata*.
- Európa Tanács (1950): *Emberi Jogok Európai Egyezménye*.
- Európa Tanács (1981): *A személyes adatok gépi feldolgozása során az egyének védelméről szóló egyezmény* (108. számú egyezmény).
- Európai Bizottság (2010): *A Bizottság közleménye az Európai Parlamentnek, a Tanácsnak, a Gazdasági és Szociális Bizottságnak és a Régiók Bizottságának – A személyes adatok európai unión belüli védelmének átfogó megközelítése*. COM(2010) 609 végleges.
- Európai Bizottság (2012): *Javaslat – Az Európai Parlament és a Tanács rendelete a személyes adatok feldolgozása vonatkozásában az egyének védelméről és az ilyen adatok szabad áramlásáról (általános adatvédelmi rendelet)*. COM(2012) 11 végleges.
- 29. cikk szerinti adatvédelmi munkacsoport (2014): *06/2014. számú vélemény az adatkezelő 95/46/EK irányelv 7. cikke szerinti jogszerű érdekeinek fogalmáról*. 844/14/HU, WP 217.

Alkotmánybírósági és NAIH határozatok:

- 8/1990. (IV. 23.) AB határozat
- 20/1990. (X. 4.) AB határozat
- 15/1991. (IV. 13.) AB határozat
- 470/B/2006. AB határozat
- 192/2010. (XI. 18.) AB határozat
- NAIH/2019/2668/2 határozat (előzmény: NAIH/2018/5457/V)

Ábrák és táblázatok jegyzéke

Ábrák:

Táblázatok: