

Stricz Walter Roland

joghallgató

Szégedi Tudományegyetem, Állam- és Jogtudományi Kar

A JOGSZERŰ ADATKEZELÉS A GDPR RENDELET UTÁN*

Debreceni Jogi Műhely, 2019. évi (XVI. évfolyam) 3-4. szám (2019. december 31.)

DOI 10.24169/DJM/2019/3-4/3

The Right to Information Self-Determination after the General Data Protection Regulation – Summary

Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), became effective on 25 May 2018. With the regulatory form the legislator raised the regulation of the right to the protection of personal data within the European Union to a higher level. The legislative act has a fundamental impact on the legal systems of the member states showing various differences from each other. Further, it can be stated as a general experience that the right to the protection of personal data and the nature of such right are less known either to those affected or to the data controllers. The new legislative act and the penalties with increased amounts [Article 84 of the GDPR] demand the elaboration of a study understandable for laics, too. Finally, as a result of the General Data Protection Regulation, the institution system ensuring the protection of personal data has fundamentally changed, so, therefore, it is also necessary to examine the authorities of the member states and the Union, as well.

The study primarily approaches the occurring problems from the practice side. Accordingly, the examination conducted by the Commission nationale de l'informatique et des libertés (CNIL) against Google is described, as the first significant penalty imposed based on the General Data Protection Regulation.

The first part of the study is intended to present the right to the general protection of personal data. The historical part addresses in details the major elements of the historical development of data protection and the development of its contents, with particular regard to the appearance of the right to information self-determination based on the so-called “census-judgement” of 1983 of the BVerfG (Federal Constitutional Court of Germany). Finally, this part touches upon the theories defined in connection with the historical generations of the right to the protection of personal data. After the historical part the study addresses the peculiarities of the right to the protection of personal data, paying particular attention to separation from the neighbouring legal areas.

The second part is intended to present the prevalence of the right to information self-determination according to the GDPR. It is the institution system protecting personal data that has undergone the most significant change. The Work Group under Article 29 has been replaced by the Data Protection Agency set up based on the GDPR. Setting up the Agency, enlarging its scope of authority and its stronger independence from the executive powers of the Union can, by all means, be evaluated positively. As regards the security of personal data, the practice, major directives and opinions of the Work Group under Article 29 have been examined. It is a significant step forward that the GDPR has made the sphere of special personal data more specific, promoting by this the increase of the extent of protection. It is



* „Az Emberi Erőforrások Minisztériuma UNKP-18-2 kódszámú Új Nemzeti Kiválóság Programjának támogatásával készült.”

Témavezető: Prof. Dr. Görög Márta.

important that, as a general rule, the Regulation forbids controlling special personal data. The definition of the concept of personal data is an essential condition for understanding the regulation. In addition to the principles of controlling personal data, the legal fundamentals of data control have particular significance, with special regard to the consent and the data control necessary for performing the contract. In my view, the consent is a legal fundament of auxiliary nature for data control, which is also supported by the opinions of the Work Group, too. Granting the consent and the individual excluding circumstances occurring in connection with this, were examined on a case-by-case basis. In my opinion, the automated decision making process and the regulation of profile creation are one of the most cardinal issues of the GDPR. The way in which profiles are created, their use and the permissibility of such use are discussed in details. In my view, the regulation of the GDPR is deficient as regards the automated decision making process and the profile creation. The decision making necessary for performing the contract is not separated sharply enough, and it is not necessary for this. In my opinion, in respect of this latter sphere of cases the GDPR is not strict enough and may easily serve as a basis for misuse on the part of data controllers. In my view, granting the consent should be made stricter in respect of creating profiles and the introduction of the (contradictable) legal presumption of refusal would also be desirous.

Előszó

2018. május 25-én hatályba lépett az Európai Parlament és a Tanács általános adatvédelmi rendelete (a továbbiakban: GDPR), amely alapvető változásokat hozott az adatvédelem szabályozási területén, mind uniós, mind pedig magyar szinten. Jelen tanulmánynak az a legfőbb célja, hogy az Olvasóval a teljesség igénye nélkül megismertesse a személyes adatok védelméhez való jog természetét és érvényesülésének alapjait, valamint GDPR által meghatározott jogi környezet jellegét és sajátosságait.

Az Európai Unió adatvédelmi reformcsomagja jelentős hatást gyakorolt mind uniós, mint tagállami szinten, így a tanulmány során külön utalni fogok a magyar jogi sajátosságokra. Mindezeket túlmenően fontosnak tartom a GDPR alá vont alanyi kör válaszreakcióit azt, hogy miként próbálnak megfelelni az jelenlegi előírásoknak.

Bevezetés

2019. január 22. napja olyannak ígérkezett, mint a többi tél végi nap. Az emberek időnként lopva kitekingettek a jégvirágos ablakokon a tavasz hírnökeit keresve, de bánatosan kellett tudomásul venniük, hogy a tél még nem ért véget. A hideg idő még legalább egy hónapig kitart, és ez a megállapítás sokakban azt a látszatot kelthette, hogy a jelenlegi nap is csak egy a sok unalmas, didergős, feladatokkal teli keddi nap közül. Rövidesen azonban a médiában egy új hír röppent fel és szerzett magának mind nagyobb érdeklődést, ez a hír pedig nem volt más, mint hogy „50 millió eurós bírságot kapott a Google”.¹

Az olvasók többsége elsőre minden bizonnyal közönyösen olvasta a hírt, hiszen mindennapos, hogy valamelyik technológiai óriást megbüntessék valamilyen versenyt torzító, vagy szabadalmat sértő tevékenysége miatt. A jelenlegi büntetés viszont más volt. Ezt a GDPR, az Európai Unió általános adatvédelmi rendeletének megsértése miatt szabták ki. A fenti mozaikszó minden bizonnyal ismerősen csengett az olvasók többségének, hiszen a hivatkozott rendelet 2018. május 25-i hatályba lépését megelőzően - és azt követően is - tömve volt az internet a közelgő új adatvédelmi szabályozás életbe lépéséről. Bár ez valószínűleg a többségnek bosszúságot jelentet, amiért a gondtalan szörfözést megzavarta egy újabb felugró ablak, amelyet be kellett zárni. Az érdeklődőbb szemlélők ugyanakkor utána olvashattak, hogy mit is tartalmaz az eljövendő szabályozás, de a jogi terminus technikusokkal teletűzdelt rendelet még a legszántabbak kitartását is próbára tehet.

Itt volt ugyanakkor ez az ötven millió euró, ami nem kis összeg - mintegy tizenhatmilliárd forint - és korábban ilyen címen senki sem kapott ilyen nagy büntetést. Az említett marasztalás az eddigi legnagyobb

¹ <https://www.hwsz.hu/hirek/59894/gdpr-cnll-adatvedelmi-hatosag-google-buntetes.html> (2019.03.12.)

bírság, amelyet a francia adatvédelmi hivatal² (a továbbiakban: CNIL) a szabott ki a GDPR több pontjának megsértése miatt. A hivatalos indokolás szerint a büntetést azért szabta ki a CNIL, mert „a Google-fiókok létrehozása során a cég nem közli értelmeiben, hogy milyen adatokat fog feldolgozni, és nem elég egyértelmű a személyre szabott hirdetések jogalapja sem.”³

A tanulmányhoz kellemes olvasást kívánok!

A szerző

I. fejezet – Az információs önrendelkezési jog és környezete

Jelen fejezet célja - az Előszóban meghatározottakkal összefüggésben - az adatvédelemhez való jog történeti fejlődésének, valamint természetének a bemutatása. A tanulmány megírása során fontos szempont volt a jogintézmény jogi környezetének átfogó bemutatása az olvasói interpretáció elősegítése érdekében.

1. Történeti rész

1.1. A tételes jogi szabályozás megjelenését megelőző időszak

A személyes adatok gyűjtése egyidős a szervezett emberi közösségek megjelenésével, ami az Ókor kezdetére tehető. Az adatgyűjtési tevékenység megkezdésének kiváltó okai a szervezett közösségeken belüli munkamegosztásban, valamint - a mai napig hatóan - az adóztatás alapjának megteremtésében jelölhető meg. Az írott történelem egyik első ismert átfogó adatgyűjtését még Augustus császár rendelte el Jézus születését megelőzően,⁴ de az érett középkori Európából is ismert népösszeírás.⁵

„Az adatvédelmi jog megjelenése előtti korszakra még nem volt jellemző az elektronikus adattároló és –feldolgozó rendszerek tömeges alkalmazása. A személyes adatok összekapcsolásának, feldolgozásának, a személyiséget kiszolgáltató helyzetbe hozó személyiségprofil megalkotásának az esélye ekkor még csekély volt, mivel az ilyen tevékenység csak igen nagy ráfordítás mellett volt végezhető.”⁶ A technológiai fejlődés ugyanakkor egyre inkább lehetővé tette a személyes adatok egyre átfogóbb gyűjtését. Az ezzel kapcsolatos félelmek az irodalomban is megjelentek többek között George Orwell 1984 című, a szerző által elképzelt jövőbeli világot bemutató regényében.⁷

A XX. század első felének háborúi és az azokat követő jelentős mértékű gazdasági, politikai és társadalmi átrendeződések során a hatalom birtokosai permanens módon felhasználták a természetes személyek személyes adatait politikai céljaik megvalósításához. A vallásfelekezeti-, valamint az etnikai hovatartozással kapcsolatos adatokat felhasználva került sor a zsidóság gettósítására, valamint a háborút követően a német kisebbség kitelepítésére is (1946-48). A II. világháború borzalmi ráébresztették az európai államokat az emberi jogok nemzetközi védelme megteremtésének szükségességére. Az érintett emberi jogok eklatáns példája volt többek között a személyes adatok védelméhez való jog. Mindezek ellenére a háborút követő emberi jogi kodifikációk, így *expressis verbis* sem az Európa Tanács keretében elfogadott Emberi Jogok Európai Egyezménye,⁸ sem az ENSZ Közgyűlése által elfogadott Polgári és Politikai Jogok Nemzetközi Egyezségokmánya⁹ nem tartalmazta a személyes adatok védelméhez fűződő jogot. A személyes adatok védelméhez való jog jogszabályi szabályozására egészen a XX. század második feléig kellett várni.

² Commission nationale de l'informatique et des libertés (CNIL)

³ <https://www.hsw.hu/hirek/59894/gdpr-cnil-adatvedelmi-hatosag-google-buntetes.html> (2019.03.12.)

⁴ „Azokban a napokban történt, hogy Augustus császár rendeletet adott ki, hogy az egész földkerekséget írják össze” BIBLIA, Lukács evangéliuma 2. fejezet 1. vers

⁵ Az első angol népszámlálás a Domesday Book (1086) volt, amelynek megalkotását „Hódító Vilmos a Gloucesterben 1085 karácsonya táján tartott witan előtt jelentett be”. RUSZOLY József: *Európai jog- és alkotmánytörténelem*, Pólay Elemér Alapítvány Szeged, 2013. 362.

⁶ JÓRI András – SOÓS Andrea Klára – BÁRTFAI Zsolt – HÁRI Anita: *A GDPR magyarázata*, Hvg-Orac Lap- és Könyvkiadó Kft., Budapest, 2018. 27.

⁷ JÓRI, 2018.28.

⁸ Convention for the Protection of Human Rights and Fundamental Freedoms (Róma, 1950. november 4.)

⁹ International Covenant on Civil and Political Rights (New York, 1966. december 16.)

1.2. Az adatvédelmi jog európai fejlődésének főbb állomásai

A történeti rész bemutatása során a tanulmány példálózó felsorolást követ, nem kerül valamennyi adatvédelemmel kapcsolatban elfogadott szabályozás említésre. A kronológiai sorral párhuzamosan törekszem a minél magasabb fokú adatvédelmi integráció felé haladva bemutatni a főbb történeti jogszabályokat.

Az előbbiekben kifejtett történelmi fejlődés alapján megállapítható, hogy az adatvédelemhez való jog egy relatíve fiatal jogterület, szemben mondjuk az tulajdonhoz való joggal, melyet már az Emberi és Polgári Jogok Nyilatkozata¹⁰ is magába foglalt. Az első adatvédelmi szabályozást *Hessen tartományi kormánya* fogadta el 1970-ben, ezt követte a Svédország 1976-ban megalkotott szabályozás, továbbá a Németországban a szövetségi szintű törvény 1976-ban.¹¹ Szembetűnő, hogy a huszadik század negyvenes éveire kiteljesedő adatvédelmi problémák és a jogterület szabályozására vonatkozó igények ellenére az adatvédelmi tárgyú jogszabályok első generációjának megalkotására csupán harminc évvel később, a hetvenes folyamán került sor.

A kezdeti nemzeti szabályozások megszületését követően megkezdődött az adatvédelemhez való jog nemzetközi szintű szabályozásának megteremtése is. Elsőként az a Gazdasági Együttműködési és Fejlesztési Szervezet (OECD) keretében fogadták el az *OECD-irányelvek a magánélet védelméről és a személyes adatok határon átvélt áramlásáról*¹² szövegű nemzetközi egyezményt (a továbbiakban OECD-irányelvek). Az irányelvek között rögzített adatvédelmi alapelvek megtalálhatók napjaink meghatározó adatvédelmi szabályozásában a GDPR-ban¹³ is, így többek között az irányelvek elvi tételei kimondják az adattakarékosság elvét, a pontosság elvét, vagy a célhoz kötöttség elvét is. Az OECD keretében elfogadott irányelvek jelentőségének másik lába dimenziója, hogy több, a későbbiekben elfogadott nemzetközi egyezménnyel szemben az irányelveknek az OECD tagállamai miatt - az Európán kívüli térségből - részese az Amerikai Egyesült Államok és Ausztrália is.¹⁴

Az OECD-irányelvek elfogadását követően 1983-ban került sor az immár tisztán európainak mondható, *az egyének védelméről a személyes adatok gépi feldolgozása során* elnevezésű Európa tanácsi adatvédelmi egyezmény (a továbbiakban ET-egyezmény) elfogadására.¹⁵ Az ET-egyezmény hatálya kiterjed többek között „a személyes adatok automatizált állományaira és a személyes adatok gépi feldolgozása során a köz- és a magánszektorban.”¹⁶ A szerződés lehetőséget biztosít a részes felek számára, hogy az egyezmény hatályát további tárgykörökre is kiterjesszék.¹⁷ Az ET-egyezmény kapcsán fontos kiemelni azt a körülményt, hogy az Európai Bizottság az Európa Tanács keretében megvalósult egyezmény mellett nem kívánt külön közösségi jogi normát alkotni az személyes adatok védelméről, hanem ösztönözni próbálta a Közösségek tagállamait, hogy csatlakozzanak az ET-egyezményhez.¹⁸ Az Európai Bizottság hozzáállása következtében partikulárisra vált az adatvédelemhez való jog „európai” szabályozása, így teremtve meg az igényt egy önálló uniós szabályozásra.

Kiemelt jelentőséggel bírt a német Alkotmánybíróság (a továbbiakban: BVerfG) 1983-as ún. „népszámlálás-ítélet”,¹⁹ ugyanis a BVerfG ebben a döntésében határozta meg az információs önrendelkezéshez való jogot. A BVerfG elvi érvelésében mondta ki a fenti ítéletében, hogy az érintett személy alapvető joga, hogy

¹⁰ Déclaration des droits de l'homme et du citoyen (Az Alkotmányozó Nemzetgyűlés 1789. augusztus 26-án fogadta el.)

¹¹ PÉTERFALVI Attila – RÉVÉSZ Balázs – BUZÁS Péter: *Magyarúzat a GDPR-ról*, Wolters Kluwer Kft., Budapest, 2018. 25.

¹² Guidelines on the Protection of Privacy and Transborder Flows of Personal Data

¹³ 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).

¹⁴ JÓRI, 2018. 34.

¹⁵ PÉTERFALVI, 2018. 25.

¹⁶ ET-egyezmény 3. cikk 1.

¹⁷ ET-egyezmény 3. cikk 2.

¹⁸ JÓRI, 2018. 36.

¹⁹ „Volkszählungsurteil” Az eredeti német szöveg nem hivatalos magyar fordítása In: TÓTH Zoltán (szerk.): *Informatika-Jog-Közigazgatás – Nemzetközi dokumentumok I.*, InfoFilia, Budapest, 1991. 6.1-6.39.

személyes adatai felett a rendelkezési jogát gyakorolja. Az ítélet olyan történelmi kontextusban született meg, amelyben a korábbi manuális adatfeldolgozási folyamatokat elkezdte felváltani az automatizált technológia. Az azonnali adattovábbítás lehetőséget biztosított az érintetthez tartozó egyes személyes adatok rövid időn belüli összekapcsolására anélkül, hogy azok pontosságát, valóságát az érintett személy ellenőrizni lenne képes. Az ítélet igazi jelentősége abban áll, hogy elsőként határozta meg és vezette le az információs önrendelkezési jogot, amelynek korábban partikuláris módon volt jelen a megelőző jogforrásokban. A későbbiekben az személyes adatok védelméhez való jog természetének ismertetése kapcsán a tanulmány konkrétan ki fog térni a BVerfG megállapításaira.²⁰

Az adatvédelmi szabályozás következő fontos lépését az Európai Unió *adatvédelmi irányelve*²¹ (a továbbiakban: Irányelv) jelentette. Az 1995-ös Irányelv jelentette az első uniós szintű szabályozást ugyanakkor fontos kiemelni a ianus arcú természetét. Az Irányelv deklarálja minden természetes személy számára a személyes adatok védelméhez való jogot, viszont ezzel párhuzamosan az Európai Unió keretén belül a belső piac szabad működését és - a belső piac keretében - a személyes adatok szabad áramlását is biztosítani kívánja.²² A szabad adatáramlás és e mellett a természetes személyek megfelelő védelme nem szükségképpen ellentétes egymással. Amennyiben megteremtésre kerül a személyes adatok kezelésének megfelelő szintű védelme, és ezen belül az adattovábbítás ellenőrzése is az előbbi paradox helyzet feloldható. Az Irányelv esetében ezt még nem sikerült megvalósítani mivel az Irányelv preambulum egyfelől kijelenti, hogy „össze kell hangolni a tagállamok jogszabályait ahhoz, hogy biztosított legyen a személyes adatok határokon keresztül történő áramlását”,²³ másrészt azt is rögzíti, hogy a „jogszabályok közelítése nem vezethet az általuk nyújtott védelem szintjének csökkenéséhez.”²⁴ Többek között a fenti okok miatt is vált szükségessé az általános adatvédelmi rendelet megalkotása, amely részben arra is hivatott, hogy a fenti oximoront feloldja,²⁵ viszont a GDPR részletesebb ismertetésére a későbbiekben fog sor kerülni.

A magyar jogi szabályozás fejlődésnek részletes bemutatására nem tárgya jelen tanulmánynak, mivel döntően követte az európai és a bővebb értelemben vett nemzetközi trendeket. Mindezek ellenére a magyar jogi szabályozás is érezte hatását a nemzetközi környezetben, ily módon a magyar jogásztársadalom is fel tud mutatni hozzáadott értéket az adatvédelemhez való jog fejlődése tekintetében. Hegedűs kifejti, hogy az 1980-as években indult adatvédelmi tárgyú magyar kutatások nyomán kialakult az a nézet, hogy az adatvédelemhez való jog párja, ha úgy tetszik ellenpólusa az információs szabadság, és a kutatók megállapítása szerint ez a két jogterület alkotja egységesen az információs jogokat. Az első magyar adatvédelmi törvény²⁶ is ezt a szemléletet követi, és egy jogszabályon belül, közösen szabályozza az egyéneket megillető adatvédelmet és az állammal szemben érvényesíthető információs szabadságot. A magyar jogászok kutatásának minőségét jelzi, hogy a törvény elfogadását követő években több állam is átvette a kettős szabályozás modelljét.²⁷

1.3. Az adatvédelmi jog generációi

Az adatvédelmi tárgyú szabályozás korszakolására vonatkozóan többféle elmélet is kifejtésre került. Az egyes szerzők által megalkotott elméletek részben fedik egymást, és a megelőző történelmi részben is tárgyalt valamely főbb jogalkotási termékhez kötik az egyes generációk határait. Közösnek mondható, hogy döntően három-, négy korszakra osztják az adatvédelmi szabályozást, oda nem sorolva a tételes jogi rendelkezéseket megelőző időszakot.

Mayer-Schönberger négy fő korszakot különít el egymástól. Az elsőben a szabályozást még a technológiafüggőség jellemzi; a második korszakban már egyre hangsúlyosabban jelennek meg az egyének jogai. A harmadik korszakot a korábban már említett német „népszámlálás-ítélet” és a nyomán

²⁰ JÓRI, 2018. 32.

²¹ 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

²² Irányelv 1. cikk, valamint az (1)-(5) preambulumbekendések

²³ Irányelv (8) preambulumbekendés

²⁴ Irányelv (10) preambulumbekendés

²⁵ GDPR (5) és (7) preambulumbekendés

²⁶ 1992. évi LXIII. törvény a személyes adatok védelméről és a közérdekű adatok nyilvánosságáról

²⁷ LAMM Vanda: *Emberi jogi enciklopédia*, Hvg-Orac Lap- és Könyvkiadó Kft., Budapest, 2018. 14.

kibontakozó információs önrendelkezési jogi koncepció határozza meg. A végső generációt pedig a lefektetett absztrakt alapokon túl, a szektoralitás, a korábbi általános szabályozás konkretizálása jellemzi.²⁸

Eltérő álláspontot fogalmaz meg Majtényi, aki három fő generációt különít el egymástól. *Majtényi* az első generáció jellemzőjeként a részben automatizált adatkezelésre irányuló szabályozást jelölte meg. A középső korszakban a szabályozás már független az áró részben automatizáltadathordozóktól. A jelenleg is tartó korszakban véleménye szerint a fő szerep az integrációé.²⁹

A *Jóri* szerzőkvartert szintén három korszakot határol el, amelyek esetében a korszakhatárokat a német adatvédelmi jogfejlődés főbb pontjaihoz kötik. Ily módon elhatárolást jelent a népszámlálás-ítélet és az újabb adatvédelmi szabályozás³⁰ elfogadása.

A szerzők megállapítása szerint az első generációs adatvédelmi szabályozások még az egyén autonómiájába történő állami behatolástól való félelem eredményeként kerültek megalkotásra. Az 1960-70-es években a számítógépes részben automatizált, számítógépes adatkezelés szabályozása volt a jogalkotó célja, amelyre Majtényi is utalt a saját korszakolása kapcsán. Ki kell emelni ugyanakkor, hogy ebben az időszakban még nem került megállapításra az információs önrendelkezési jog, így csak egyes részjogosítványai érvényesültek a korai szabályozásokban.

A második generációs adatvédelmi szabályozás nívója az információs önrendelkezési jog megállapítása volt, amelyet a BVerfG az általános személyiségi jogból vezetett le. Továbbá fontos megemlíteni, hogy a jogi szabályozást kiterjesztették az adatkezelés teljes folyamatára, valamint igyekeztek egyre magasabb szintű absztrakciót megvalósítani, kvázi univerzális szabályozást adni, viszont a nagyfokú absztrakció, és az adatkezelés szabályainak általánosítása tette szükségessé a harmadik generációs szabadságjogok megalkotását.

A harmadik generációs szabályozás tekintetében meg kell állapítani, hogy a jogalkotók egy paradigmaváltáson estek át. Míg a megelőző generációban a minél magasabb szintű absztrakció elérése és a technológiától független szabályozás megalkotása volt a cél, a harmadik generáció esetében ennek az ellenpólusa figyelhető meg. A szektorális szabályozás következtében a jogalkotók igyekeztek tipizálni a felmerülő adatkezeléseket, és ezekre speciális szabályokat alkotni, valamint a jogalkotó a technológia követése helyett igyekszik előre menni és a szabályozás által befolyásolni az adatkezelés mikéntjét.

A harmadik generáció során említett jogalkotói trendek eklatáns példája az Európai Unió adatvédelmi reformcsomagja. Mivel a szabályozás nemrég lépett hatályba a koncepció sikerével kapcsolatban az évek alatt kikristályosodó gyakorlat megvizsgálásával lehet majd biztosabb véleményeket megfogalmazni.³¹

2. A személyes adatok védelemhez való jog megítélése

Az egyes jogterületek szabályozásának mikéntjét minden esetben különböző - sokszor egymással ellentétes irányultságú - érdekek alakítják, ez alól a megállapítás alól a személyes adatok védelméhez való jog sem képez kivételt. Az adatvédelem esetében is szembeállítható egymással az érintett magánérdeke, valamint a személyes adatok megismerhetőségéhez kapcsolódó közérdek. Az általános adatvédelmi rendelet preambuluma is ezt ianus arcúságot mutatja, amikor egyfelől az Alapjogi Chartára hivatkozva deklarálja az adatvédelemhez való jog alapjogi jellegét, másrészt biztosítani kívánja az Európai Unió keretében megvalósult belső piac rentábilis működését elősegítő adatáramlást.³²

A jog sok esetben sajnálatosan nem előidézi a társadalmi és politikai folyamatokat, hanem követi azokat. Az adatvédelemhez való jog aktuális paradigmáját is döntően az aktuális igények szerint alakítják. A World Trade Center elleni terrortámadás a közérdek előretörését eredményezte, míg a Cambridge Analytica botrány a magánérdek hatványozódását vonta maga után.

²⁸ JÓRI, 2018.29.

²⁹ JÓRI, 2018. 29.

³⁰ Teledienstschutzgesetz

³¹ JÓRI, 2018. 27-47.

³² GDPR (1)-(3) preambulumbekendések

Az adatvédelemhez való jog megfelelő szabályozásának megteremtéséhez meg kell találni az érdekegyensúlyt. A paradox helyzet feloldásának elméleti hátterét a *Duncan-féle „R-U Confidentiality Map”* jelenti, amelyen a „Risk” a nyilvánosságra hozatal kockázatát, míg az „Utility” a nyilvánosságra hozott adatok használhatóságát jelzi. „*Duncan elmélete szerint a keresett pont az, ahol a nyilvánosságra hozott adatok kockázata még elviselhető, ugyanakkor a görbe növekedésének intenzitása a hasznosság irányában már nem számottevő.*”³³ Kárpáti példáját használva az adatvédelemhez való jog egyensúlya hasonlatos a két egymásra helyezett biliárdgolyóhoz, amelyeknek van egy képzeletbeli egyensúlyi holtpontja, viszont ez az állapot csak pillanatnyi jellegű.³⁴

2.1. Az adatvédelemhez való jog természete

A magyar jogforrási hierarchia csúcán az Alaptörvény helyezkedik el. Amint arról *Hegedűs* is említést tesz, az adatvédelmi jog klasszikus polgári és politikai jog,³⁵ és mint ilyet Hazánk Alaptörvénye³⁶ is deklarál a VI. cikk (1) bekezdés első fordulatóban.³⁷ Az uniós jog tekintetében az Alapjogi Charta 8. cikke és az EUMSZ 16. cikk (1) bekezdése³⁸ rögzíti a személyes adatok védelméhez való jogot, mint alapvető emberi jogot. Ugyanakkor a személyes adatok védelméhez való természetének bemutatását célszerű a német jogban kezdeni. Már korábban, a történeti részben is említésre kerül a BVerfG 1983-as népszámlálás-ítélete, amelyben elvi érveléssel mondták ki, hogy „*az Alaptörvény ennyiben biztosítja az egyén illetékességét arra, hogy személyes adatainak felfedéséről és felhasználásáról alapvetően maga rendelkezessen,*”³⁹ ezzel megfogalmazva az információs önrendelkezési jogot. A BVerfG az emberi méltóság sérthetlenségéből⁴⁰ és a személyi szabadság elvéből⁴¹ vezette le az információs önrendelkezési jogot, mint az általános személyiségi jog egyik megnyilvánulási formáját. A német döntésnek nagy hatást gyakorolt az egyes európai államok szabályozására, így a magyarra is.

Az adatvédelemhez való jogot Magyarországon a rendszerváltás során foglalták bele az Alkotmányába.⁴² A magyar Alkotmánybíróság az ún. „személyi szám”⁴³ elnevezésű döntésében fejtette ki álláspontját az információs önrendelkezési jog lényegi tartalmával kapcsolatban. Az Alkotmánybíróság indokolása alapján „*az információs önrendelkezési jog lényege az, hogy az érintett tudhatja és követheti személyes adatai felhasználásának útját és körülményeit, először is biztosítani kell e jog gyakorlásának előfeltételét*”⁴⁴, továbbá megállapítja az adatvédelemhez való jog konstitutív elemeit, amelyek a célhoz kötött, osztott információs rendszerek elve, és az a főszabály, hogy az adatot az érintettől, annak tudtával és beleegyezésével kell felvenni.⁴⁵ Az Alaptörvény hatályba lépését megelőzően meghozott döntések helyzetét maga az Alaptörvény rendezi; ugyan „*az Alaptörvény hatálybalépése előtt meghozott alkotmánybírósági határozatok hatályukat veszítik. E rendelkezés nem érinti az ezen*

³³ KÁRPÁTI József: A bizalmas adatok kezelése és a magántitok védelme In: Statisztikai Szemle, 2003. 81. évfolyam 1. szám, 71.

³⁴ Kárpáti, 2003. 70.

³⁵ LAMM, 2018. 12.

³⁶ Magyarország Alaptörvénye 2012. január 1-jétől kezdve képezi a magyar jogforrási hierarchia csúcát.

³⁷ Alaptörvény Szabadság és Felelősség rész: VI. cikk (1) „*Mindenkinek joga van ahhoz, hogy magán- és családi életét, otthonát, kapcsolattartását és jó hírnevét tiszteltben tartsák.*”

³⁸ EKSz. korábbi 286. cikke

³⁹ Népszámlálás-ítélet In: TÓTH, 1991. 6.16.

⁴⁰ Német Alaptörvény (Grundgesetz, a továbbiakban: GG) 1. cikk (1) bekezdés: „*Az emberi méltóság sérthetetlen. Annak tisztelete és védelmezése kötelező minden állami hatalom számára.*” Az eredeti német szöveg magyar fordítása In: NÉMETH Lajos (szerk.): *Nemzeti alkotmányok az Európai Unióban*, Wolters Kluwer Kft., Budapest, 2016. 661.

⁴¹ GG 2. cikk (1) bekezdés: „*Mindenkinek joga van arra, hogy saját személyiségét szabadon kibontakoztassa, amennyiben az mások jogait nem sérti és nem ütközik az alkotmányos rendbe, vagy erkölcsi törvénybe.*” Az eredeti német szöveg magyar fordítása In: NÉMETH, 2016.661.

⁴² A Magyar Köztársaság Alkotmányáról szóló 1949. évi XX. törvényt a rendszerváltás során az az 1989. évi XXXI. törvény módosította. Ezzel a módosítással ruházták fel jogállamisággal a korábban kommunista ideológián alapuló szocialista Alkotmányt. A személyes adatok védelme mellett bekerült az Alkotmányba többek között a közérdekű adatok nyilvánossága és terjeszthetősége, valamint a szabad sajtó biztosítása is.

⁴³ 15/1991. (IV. 13.) AB határozat

⁴⁴ 15/1991. (IV. 13.) AB határozat III. 2.4.

⁴⁵ 15/1991. (IV. 13.) AB határozat III. 3.1.

határozatok által kifejtett joghatásokat.⁴⁶

Fontos kiemelni, hogy más alapjogokhoz hasonlóan a személyes adatok védelméhez fűződő jog sem abszolút, nem korlátozhatatlan.⁴⁷ A GDPR preambuluma alapján az adatvédelmi jogot az arányosság elvét szem előtt tartva, a társadalomban betöltött szerepének függvényében kell figyelembe venni, egyensúlyban más alapvető jogokkal.⁴⁸ Az Alkotmánybíróság 2/1990. (II. 18.) AB határozatában megállapította, hogy *a személyes adatok védelméhez való jog nem abszolút jog*. Korlátozására kivételes esetben, törvényben kerülhet sor. Az adatvédelemhez való jog korlátozásával kapcsolatban meg kell említeni Sólyom László különvéleményét, amelyben kifejti, hogy a korlátozás abban az esetben tekinthető alkotmányosnak, ha: *„megfelel az Alkotmány 8. § (3) bekezdésében megállapított feltételeknek. [...] alapvető jog gyakorlása csak alkotmányerejű törvényben megállapított olyan korlátozásnak vehető alá, amely az állam biztonsága, a belső rend, a közbiztonság, a közegészség, a közérköls vagy mások alapvető jogainak és szabadságának védelme érdekében szükséges.”* Sólyom László különvéleményének dogmatikai alapját a BVerfG 1983-as ítélete szolgáltatja. BVerfG - a már hivatkozott népszámlálás-ítéletében - az információs önrendelkezési joggal összefüggésben kifejtette, hogy az egyénnek nem korlátlan értelemben van joga személyes adatai felett, mégpedig azért, mert *„az információ, bármennyire személyes is a társadalmi valóság olyan leképezése, amelyet nem lehet kizárólag egyedül az érintetthez tartozónak tekinteni”*.⁴⁹ Ebből következően „túlnyomó közérdek” esetén lehetséges az információs önrendelkezési jog korlátozása. A BVerfG az információs önrendelkezési jog tényleges korlátozása esetén kettős feltételrendszert állított fel. Az első feltétel, hogy a korlátozás megengedhetőségéhez szükség van egy olyan *törvényes indokra*, amelyből a korlátozás feltételei és mértéke megismerhető az érintettek felől. A másik feltétel, hogy a közhatalom csak a közérdek védelme érdekében elengedhetetlenül szükséges mértékben korlátozhatja az információ önrendelkezési jogot (*arányosság alapelve*).⁵⁰

A magyar jogalkotási termékek közül a Polgári Törvénykönyv⁵¹ (a továbbiakban Ptk.) és az információs önrendelkezési jogról és az információszabadságról szóló törvény⁵² (a továbbiakban: Infotv.) alkotják a hazai adatvédelmi szabályozás gerincét. A Ptk. a - népszámlálás-ítélettel és a személyi szám ítélettel összhangban - a nevesített személyiségi jogok között helyezi el a személyes adatok védelméhez való jogot.⁵³ A Ptk. a kódex jellegének következményeként részletes szabályozást nem foglal magába a személyes adatok védelmével kapcsolatban, pusztán a személyiségi jogokra vonatkozó általános szabályokat és a megsértésük szankcióit tartalmazza.⁵⁴ Az adatvédelemre vonatkozó részletes törvényi szabályozást az Infotv. foglalja magába, amely jelentős mértékű módosuláson esett keresztül a GDPR hatályba lépését követően. A változások mértéke ugyanakkor sok kérdést felvetet.

2.2. Elhatárolások

Minden jogterület bemutatása során szükséges megtenni a kellő elhatárolásokat a szomszédos jogterületektől, ezzel elkerülve a tanulmány szükségtelen terjengősségét. A jogterület elkülönítését követően a konkrét jogszabályokra irányuló kutatások - részben jelen tanulmány is meg kell határozni a jogterület szabályozásának azt a szegmensét, amelyre irányul, természetesen a kellően pontos bemutatás érdekében megtartva a szabályozás kontextusát. Az elhatárolás során a tanulmány fokozatosan fokozatosan közelíteni a tárgyat adatvédelmi szabályozáshoz, és meg kívánja adni az elhatárolás alapjául szolgáló ismérveket.

⁴⁶ Alaptörvény Záró és Vegyes rendelkezések 5. pont

⁴⁷ A német alkotmánybíróság részben az emberi méltóság elvéből vezette le az információs önrendelkezési jogot. A magyar Alkotmánybíróság a 64/1991. (XII. 17.) AB határozatában kimondta, hogy *„az emberi méltósághoz való jog azt jelenti, hogy van az egyén autonómiájának, önrendelkezésének egy olyan, mindenki más rendelkezése alól kivont magja, amelynél fogva - a klasszikus megfogalmazás szerint - az ember alany marad, s nem válhat eszközzé vagy tárggyá. A méltósághoz való jognak ez a felfogása különbözteti meg az embert a jogi személyektől, amelyek teljesen szabályozás alá vonhatók, nincs „érintetlen” lényegük.”* A BVerfG véleményét tükrözi a GDPR (4) preambulumbekzdése is.

⁴⁸ GDPR (1), (2) és (4) preambulumbekzdései

⁴⁹ Népszámlálás-ítélet In: TÓTH, 1991. 6.16.

⁵⁰ Népszámlálás-ítélet In: TÓTH. 1991. 6.17.

⁵¹ 2013. évi V. törvény

⁵² 2011. évi CXII. törvény

⁵³ Ptk. 2:43. § e) pont

⁵⁴ Ptk. Harmadik Könyv, Harmadik rész (Személyiségi jogok)

2.2.1. Az információs jogok elhatárolása

A korábbiakban már említésre került a magyar jogfejlődés sajátossága, nevezetesen, hogy az információs szabadságot az adatvédelemhez való jog „testvérjogának” tekintik és a két jogterület együttesen alkotja az információs jogokat. Ezen nézet nyomán alakult ki az a jogalkotói gyakorlat, amelynek keretében a két, egymással rokonítható jogterületre vonatkozó jogszabályi rendelkezéseket egy törvénybe foglalták. Mind a két jogterület az utóbbi évtizedekben jutott egyre nagyobb jelentőséghez. A jóléti államok megszületésével az állam a korábbiakhoz nem fogható mértékben kezdte el érinteni a magánfeleket. Az adatvédelem tekintetében ezzel összefüggésben az egyén magánszférájának védelme jelent meg, az információs szabadság tekintetében pedig elsősorban a közhatalom birtokosának ellenőrzése, így ez az egyik első és markáns különbség a két jogterület között.

Alapvető eltérés, hogy az adatvédelem és az információs szabadság eltérő jogokból került levezetésre. A személyes adatok védelmét az emberi méltóság sérthetlenségéből és a személyi szabadság elvéből vezette le a BVerfG.⁵⁵ Az információs szabadság viszont eredetét tekintve a véleménynyilvánítás szabadságával és a sajtószabadsággal mutat rokonságot.⁵⁶

Az egyik elsődleges megkülönböztető jegyeket a két jogterület irányultsága jelenti. Az információs szabadság *pozitív tartalmú*, mivel az államot aktív magatartásra kötelezi az *államot*, nevezetesen, hogy biztosítsa a közérdekű adatokhoz való megfelelő hozzáférést. Ezzel szemben az adatvédelemhez való jog *negatív tartalmú*, az passzív magatartásra kötelezi *az államot, illetve más adatkezelőket*. A személyes adatok védelméhez való jog biztosítottságának ellenőrzése természetesen igényel pozitív, cselekvő magatartási formákat is, viszont ezen túlmenően a szabályozás korlátokat állít az adatkezelés terjedelmére és módjára vonatkozóan. Az információs szabadság biztosítása ezzel szemben tisztán aktív magatartási formával teremthető meg. A igényt követő közigazgatási eljárás keretében megvalósuló adatszolgáltatással. Az információs szabadság biztosítása nem valósulhat meg az állam aktív részvétele nélkül, így az információs szabadság nem sorolható a klasszikus első generációs szabadságjogok közé, amelyek mindegyike az állam passzivitását igényelte. Az előbbi okokból következtében utal rá *Kerekes*, hogy a magyar terminus technikus⁵⁷ nem kellő pontosságú szemben a nemzetközi szabályozásban alkalmazott információhoz való jog terminussal (*right to information*).⁵⁸

Az elhatárolási ismérvek között kell említeni, hogy a két jogterület esetében eltérő az érintett adatok köre. Az adatvédelmi jog a természetes személyekhez szervesen kötődő személyes adatok védelmére irányul. Az információs szabadság ezzel szemben a közhatalom gyakorlása során felmerült adatokra terjed ki, amelyek adott esetben lehetnek meghatározott személyes adatok is. További fontos eltérés, hogy míg az adatvédelem csak a természetes személyeket illeti meg,⁵⁹ addig az információs szabadság a jogi személyeket is megilleti.⁶⁰

Természetesen mind az adatvédelem, mind az információs szabadság korlátozható. Sólyom László különvéleménye kapcsán már említésre kerültek a személyes adatkezelés korlátozhatóságának feltételei. Az információs szabadság is törvényi rendelkezése által korlátozható hasonlóan az adatvédelemhez. Ugyanakkor meg kell említeni egy speciális esetkört, a minősített adatok kérdését. A minősített adat védelméről szóló törvény⁶¹ értelmező rendelkezése értelmében „*közérdekű adat nyilvánosságához fűződő jogot minősítéssel korlátozni csak az e törvényben meghatározott feltételek fennállása esetén, a védelemhez szükséges minősítési szinttel és a feltétlenül*

⁵⁵ Népszámlálás-ítélet In: TÓTH, 1991. 6.16.

⁵⁶ LAMM, 2018. 405.

⁵⁷ Fontos megemlíteni, hogy nincs egységesen elfogadott elnevezése a magyarul információs szabadságnak elnevezett jognak.

⁵⁸ LAMM, 2018. 405.

⁵⁹ A GDPR a szabályozás egészében - és az elnevezésében is következetesen - a „természetes személyekkel” kapcsolatos adatkezelésről rendelkezik, valamint a (14) preambulumbekzdésben *expressis verbis* ki is mondja, hogy a rendelet hatálya nem terjed ki a jogi személyekkel kapcsolatos személyes adatkezelésre. Ennek ellenére felmerülhet, hogy a GDPR hatályán kívül elképzelhető a személyes adatok kezelése, viszont ezt egyértelműen kizárják az Infotv. - és a GDPR - értelmező rendelkezései, a személyes adat és az érintett meghatározása (Infotv. 3. § 1. és 2. pont).

⁶⁰ LAMM, 2018. 405.

⁶¹ 2009. évi CLV. törvény

szükséges ideig lehel?. A minősített adatok és a közérdekű adatok részletesebb bemutatása viszont nem célja jelen tanulmánynak.

Végezetül utalni kell az adatvédelem és az információs szabadság jogi szabályozásának szintjére. Az adatvédelem tekintetében sokkal magasabb szintű absztrakció valósult meg, valamint a GDPR hatálybalépésével az Európai Unión belül a jogszabályi környezet is döntően egységesnek mondható. Az információs szabadság tekintetében is történt nemzetállami jogalkotás,⁶² valamint elfogadásra kerültek ugyan nemzetközi egyezmények,⁶³ viszont ezek tekintetében a jogharmonizációnak csak egy alacsonyabb szintje a jogközelítés valósult meg. Az uniós szabályozás biztosítja az Európai Unió intézményeinek átláthatóságát, különös tekintettel a döntéshozó szervekre (Európai Parlament, a Tanács és a Bizottság).⁶⁴ Továbbá fontos kiemelni az ún. PSI irányelvet,⁶⁵ amely *a tagállamok számára előírta, hogy a megfelelő nemzeti jogszabályok megalkotásával biztosítsák a közszféra információinak hasznosulását.*⁶⁶

2.2.2. A jogi személyek esete

A személyes adatok védelméhez való jog, mint nevesített személyiségi jog minden természetes személyt megillető jogosultság. Felmerül ugyanakkor a nem természetes személyekkel kapcsolatos adatkezelés kérdésköre is. Fontos kiemelni, hogy személyiségi jogai csak és kizárólag a természetes személyeknek lehetnek, a jogi személyeknek ezzel szemben személyhez fűződő jogaik lehetnek. A személyhez fűződő jogok ugyanakkor sokkal szűkebbek, jellegükből adódóan nem valamennyi személyiségi jog lehet egyben személyhez fűződő jog is. Ugyanúgy, ahogy a jogi személyek nem rendelkeznek kegyeleti joggal, nem rendelkeznek a személyes adatok védelméhez való joggal sem. Az érintett és a személyes adat definíciója eleve kizárja a jogi személyeket a személyes adatok védelméhez való jog alanyi köréből, hiszen mind a kettő nélkülözhetetlen fogalmi elem a természetes személyi lét. Továbbá az általános adatvédelmi rendelet tekintetében ki kell emelni a Preambulum (2) és (14) bekezdéseit, amelyekben *expressis verbis* ki is mondja, hogy a rendelet hatálya nem terjed ki a jogi személyekkel kapcsolatos adatkezelésre.

A jogi személyek jellegéből következően szintén kizárja. Mivel a jogi személyek ún. másodlagos, származtatott jogalanyok, a létrejöttük elengedhetetlen feltétele az állami elismerés, amely a jogi személyek nyilvántartásba történő bejegyzését jelenti. A bejegyzés nélkül nem lehet jogi személyről beszélni. Ezen nyilvántartások - mint például a cégbíróságok cégnyilvántartása - esetében érvényesül a közhitelesség és a nyilvánosság elve. A jogi személyek adatainak nyilvánosságához fűződő közérdek okán ezek szabadon megismerhetőek kell, hogy legyenek.

2.2.3. A GDPR mint lex generalis

Az adatvédelmi reformcsomag esetében a GDPR tekinthető zsinórmértéknek, az adatvédelmi tárgyú szabályozások általános alapjának. Az adatvédelmi jog generációinál már kiemelésre került, hogy a harmadik generációs jogalkotás egyik fő jellemzője a szektoralitás, azaz az egyes konkrét adatkezelésekre adandó kifejezett szabályozás megalkotása. Az említett célkitűzés nem kivitelezhető anélkül, hogy ne kerülne megalkotásra egy az általános rendelkezéseket magába foglaló, magas szintű absztrakcióval rendelkező jogi norma. Az adatvédelem tekintetében ezt a szerepet a GDPR tölti be.

A mozaikszerűen felépülő szabályozásból következően megállapítható, hogy nem minden személyes adattal kapcsolatos adatkezelés tartozik a GDPR hatálya alá, így ebből következően a GDPR tárgyi hatályra vonatkozó rendelkezései jelentik az utolsó elhatárolási ismérvet.⁶⁷ A GDPR hatályát korlátozó rendelkezéseket véleményem szerint két csoportba lehet besorolni, egyrészt általános, másrészt speciális kizáró körülményekre. A speciáliskategóriába tartoznak azok az esetek, amikor egy különös jogalkotási aktus - lex specialis - érvényesül az általános adatvédelmi rendelettel szemben, míg az általános csoportba

⁶² 1966. Freedom of Information Act (USA)

⁶³ 2008. Convention on Access to Official Documents (Council of Europe)

⁶⁴ Az Európai Parlament és a Tanács 1049/2001/EK rendelete (2001. május 30.) az Európai Parlament, a Tanács és a Bizottság dokumentumaihoz való nyilvános hozzáféréstől

⁶⁵ Az Európai Parlament és a Tanács 2003/98/EK irányelve (2003. november 17.) a közszféra információinak további felhasználásáról

⁶⁶ LAMM, 2018. 410-411.

⁶⁷ GDPR 2. cikk

tartoznak az egyéb kizáró körülmények. A speciális kategória tekintetében meg kell említeni a - GDPR mellett a szűkebb értelemben vett adatvédelmi reform keretében megalkotott - bünygi adatkezeléssel kapcsolatos irányelvet⁶⁸ (a továbbiakban: Bünygi irányelv). Jelenleg további különös jogalkotási aktus jelentenek Európai Unió intézményrendszere tekintetében megvalósuló személyes adatkezelést meghatározó rendelet,⁶⁹ valamint az elektronikus hírközlési ágazatban végrehajtott adatkezelést,⁷⁰ és az elektronikus kereskedelem során felmerülő adatkezelést szabályozó irányelvek.⁷¹ Az általános kategória vonatkozásában a GDPR által nevesített kizáró ok, az uniós jog hatályán kívül eső adatkezelés, a háztartási adatkezelés,⁷² valamint a tagállamok közös kül- és biztonságpolitikával kapcsolatos adatkezelése.

Az adatvédelem uniós szintű megreformálása továbbra sem ért véget. A Bizottság az említett speciális jogszabályok tekintetében is elhatározta a felülvizsgálatot. Az általam bővebb értelemben vett adatvédelmi reformcsomaghoz tartozik 45/2001/EK rendelete és 2002/58/EK irányelve megújítása is. Mind a két felülvizsgálni kívánt terület tekintetében elmondható, hogy az új szabályozást rendeleti szinten kívánják megalkotni.⁷³ Meglátásom szerint a bővebb értelemben vett adatvédelmi reformcsomagba beletartozik a harmadik generációs adatvédelmi szabályozás szerint megvalósuló valamennyi új jogalkotási termék. Összességében megállapítható, hogy az adatvédelmi jog szabályozása igen magas harmonizációs szintet ért már el, és ez a tendencia folytatódni látszik a fentiekben is említett új adatvédelmi tárgyú tervezetekkel. Az új uniós jogalkotással megvalósuló jogegységesítés egyik mellékhatása, hogy a tagállami jogalkotók szinte teljes egészében elveszítik a jogalkotási kompetenciáikat. Mérlegelve viszont azt a körülményt, hogy mekkora előnyök származnak az egységes, magas színvonalú uniós szabályozásból mind közvetlenül a természetes személyek oldalán, mind közvetett oldalon az uniós belső piac és a versenyképesség oldalán, jelen álláspontom szerint kifizetődő.

3. Az uniós jog és a magyar jogrendszer kapcsolata

A szabályozás ismertetése előtt célszerű felvázolni az uniós jog kapcsolatát a magyar jogrendszerrel. Az Alaptörvény Q) cikke értelmében a magyar jogrendszer a monista és a dualista elmélet közül az utóbbit követi. A dualista jogrendszerekben a nemzetközi jogi normák nem kerülnek be automatikusan a belső jogrendszerbe, hanem azokat egy további jogalkotói aktussal kell transzformálni a belső jogba. Az Alkotmánybíróság két meghatározó határozatában fejtette ki az álláspontját az uniós jog megítéléséről. Az 1053/E/2005. AB határozat kijelentette, hogy „szereződési eredetük dacára, az Európai Unió alapító és módosító szerződéseit nem nemzetközi szerződésként kívánja kezelni”. Ehhez hasonló az előbbi megerősítő megállapítást tett Alkotmánybíróság a 72/2006. (XII.15) AB határozatban: „e szerződések, mint elsődleges jogforrások, és az Irányelv, mint másodlagos jogforrás, közösségi jogként a belső jog részei, mivel a Magyar Köztársaság 2004. május 1-jétől az Európai Unió tagja. Az Alkotmánybíróság hatáskörének szempontjából a közösségi jog nem minősül az Alkotmány 7.§ (1) bekezdésében meghatározott nemzetközi jognak.”⁷⁴ Ennél a pontnál meg kell említeni, noha az

⁶⁸ Az Európai Parlament és a Tanács (EU) 2016/680 irányelve (2016. április 27) a személyes adatoknak az illetékes hatóságok által a bűncselekmények megelőzése, nyomozása, felderítése, a vádeljárás lefolytatása vagy büntetőjogi szankciók végrehajtása céljából végzett kezelése tekintetében a természetes személyek védelméről és az ilyen adatok szabad áramlásáról, valamint a 2008/977/IB tanácsi kerethatározat hatályon kívül helyezéséről

⁶⁹ Az Európai Parlament és a Tanács 45/2001/EK rendelete (2000. december 18.) a személyes adatok közösségi intézmények és szervek által történő feldolgozása tekintetében az egyének védelméről, valamint az ilyen adatok szabad áramlásáról

⁷⁰ Az Európai Parlament és a Tanács 2002/58/EK irányelve (2002. július 12.) az elektronikus hírközlési ágazatban a személyes adatok kezeléséről, feldolgozásáról és a magánélet védelméről (Elektronikus hírközlési adatvédelmi irányelv)

⁷¹ Az Európai Parlament és a Tanács 2000/31/EK irányelve (2000. június 8.) a belső piacon az információs társadalommal összefüggő szolgáltatások, különösen az elektronikus kereskedelem, egyes jogi vonatkozásairól (Elektronikus kereskedelemről szóló irányelv)

⁷² A háztartási adatkezelés kritériuma, hogy az adatkezelő a személyes adatok kezelését személyes vagy otthoni tevékenység keretében végezze úgy, hogy az nem irányulhat semmilyen szakmai vagy üzleti tevékenységre In.: GDPR 2. cikk (2) bekezdés c) pont, valamint a (18) preambulumbekkezdés

⁷³ PÉTERFALVI, 2018. 32-34.

⁷⁴ BLUTMAN László: *Az Európai Unió joga a gyakorlatban – Második átdolgozott kiadás*, Hvg-Orac Lap- és Könyvkiadó Kft., Budapest, 2013. 69-70.

Alkotmánybíróság Alaptörvényt megelőző határozatai 2012. január 1.-jével hatályukat veszítették az Alaptörvény Záró és Vegyes rendelkezések 5. pontja értelmében „*e rendelkezés nem érinti az ezen határozatok által kifejtett joghatásokat*”. A fenti AB határozatok megállapították, hogy az uniós jog a nemzetközi jogtól különálló jogrendszert alkot, ezáltal az uniós jog eltérően ítélendő meg a nemzetközi jogtól.

Az uniós jog és a magyar jogrendszer közötti kapcsolat kérdésében, és így közvetve a GDPR esetében is kiemelt jelentőséggel bír az Európa-klauzula,⁷⁵ amely egyrészt előfeltétele volt hazánk uniós csatlakozásának, valamint alapul szolgál Magyarországnak és az Unió jogának az összeegyeztetéséhez.⁷⁶ Az Alaptörvény megfogalmazása szerint Magyarország az Alaptörvényből eredő egyes hatásköreit a többi tagállammal közösen, az Európai Unió intézményei útján gyakorolhatja. Problémás a kérdéskör megítélése ugyanis az államok, köztük Magyarország is *summa potestas*,⁷⁷ tehát a legfőbb hatalom hordozói. A meghatározáshoz társuló probléma, hogy elvben a szuverén államok tekintetében nem lehet felettes jogalkotóról beszélni, valamint a szuverenitás is egységes, nem megosztható. A magyar jogalkotó megfogalmazása is azt mutatja, hogy az ország nem adta át a szuverenitás egy részét, hanem csak az abból származó hatáskörök meghatározott részét kívánja közösen gyakorolni az Unió intézményeivel és a többi tagállammal. Nem eldöntött a kérdés, hogy az uniós jog milyen mértékben előzi meg a tagállami jogokat, maguk a tagállamok is eltérő állásfoglalásokat alakítottak ki. A magyar Alkotmánybíróság a közös hatáskörgyakorlás két fő korlátját állapítja meg. Egyrészt a közös hatáskörgyakorlás nem sértheti Magyarország szuverenitását (szuverenitáskontroll), másrészt nem járhat az alkotmányos önazonosság sérelmével (identitáskontroll).⁷⁸ Az Alkotmánybíróság hivatkozik a BVerfG a „*Solange-határozatokban*” kifejtett álláspontjára, amely kifejti, hogy *az Európai Unió az alapvető jogoknak többnyire a nemzeti alkotmányok által biztosított szintjével azonos, vagy legalább kielégítő mértékű védelmét képes biztosítani. Az Alkotmánybíróság ugyanakkor nem mondhat le az emberi méltóság és az alapvető jogok lényeges tartalmának ultima ratio jellegű védelméről, és biztosítania kell, hogy az Alaptörvény E) cikke (2) bekezdése alapján megvalósuló közös hatáskörgyakorlás nem jár az emberi méltóság vagy más alapvető jogok lényeges tartalmának sérelmével.*⁷⁹

Az Unió többféle jogalkotási aktust bocsáthat ki (ilyen a rendelet, irányelv és a határozat). Eltérő megkötést jelentenek a tagállamok számára, és nem egyformán engedik az eltérést vagy az alkalmazás megtörténtét. Az uniós jogharmonizációnak öt fő eszköze van, a jelenlegi kérdéskör vizsgálatánál ezek közül kettő bír jelentőséggel, a jogközelítés és a jogegységesítés⁸⁰. A jogközelítés jellemzően irányelvvel⁸¹ történik, amely megállapítja a szabályozás lényegesebb sarokpontjait és főbb irányait, valamint mintát ad a tagállamok számára. A tagállami belső jogba való implementálás viszont már a tagállamok kötelezettsége. Az átültetés során a tagállamok bizonyos mértékben eltérhetnek az irányelvtől, de a főbb kérdésekben kötelesek azt követni.⁸² A személyes adatokra vonatkozó uniós szintű szabályozást 2018. május 25-től a GDPR a korábbi irányelvi szintű szabályozástól eltérően már a jogharmonizáció egy magasabb szintjét, a jogegységesítést valósítja meg. Az EUMSZ 288. cikke alapján a rendelet általános hatállyal bír, teljes

⁷⁵ A Magyar Köztársaság Alkotmányáról szóló 1949. évi XX. törvény módosításáról szóló 2002. évi LXI. törvény illesztette be a 2/A.§-t a régi Alkotmányba.

⁷⁶ Jelenleg az Alaptörvény E) cikke tartalmazza az Európa-klauzulát, amely az Alaptörvény hetedik módosításával (2018. június 28.) nyerte el jelenleg is hatályos szövegét.

⁷⁷ Eredeti szövegén a következőképpen szól: „*maiestas est summa in cives ac subditos legibus soluta potestas*”. Jean Bodin meghatározása alapján a szuverenitás nem más, mint abszolút és állandó hatalom. WALKER, Neil: *Sovereignty in Transition*, Hart Publishing, 2006. 247-248.

⁷⁸ 22/2016. (XII.5.) AB határozat [54] bekezdése

⁷⁹ 22/2016. (XII.5.) AB határozat [49] bekezdése

⁸⁰ További jogharmonizációs eszköz a kölcsönös elismerés, a koordinációs-kiegészítő szabályozás, és az uniós szintű tevékenység szabályozása.

⁸¹ Fontos eltérés a rendeletekhez képest, hogy magánszemélyekre nézve közvetlen kötelezettséget nem állapíthat meg. A tagállamokat kötelezi, és így közvetve jelentkezik a szabályozás a magánszemélyek szintjén. Az irányelvek a szabályozási tárgyra vonatkozó alapvető rendelkezéseket, illetve az elérendő jogalkotási célokat határozzák meg. BLUTMAN, 2013. 262.

⁸² Egy irányelv nem feltétlenül kötelez minden tagállamot, adódhat olyan eset is, hogy egy vagy több tagállam az irányelv hatályán kívül esik. Ilyen például a 2011/95/EU irányelv, amely esetében „Az EUSZ-hez és EUMSZ-hez csatolt, Dánia helyzetéről szóló 22. jegyzőkönyv 1. és 2. cikkével összhangban Dánia nem vesz részt ennek az irányelvnek az elfogadásában, az rá nézve nem kötelező és nem alkalmazandó.

egészében kötelező és közvetlenül alkalmazandó valamennyi tagállamban.⁸³ A tagállamok nem módosíthatnak a rendelet tartalmán,⁸⁴ és nincs szükség semmilyen további belső jogi aktusra, hogy a tagállami jog részévé váljon, ily módon a tagállamoknak kihirdetni is tilos őket.⁸⁵

A rendeletek mindazonáltal eltéréseket biztosíthatnak a saját szabályanyaguktól, de az erre irányuló felhatalmazást *expressis verbis* tartalmazniuk kell. A Rendelet (8) és (10) preambulumbekendései rögzítik az eltérés lehetőségét a tagállamok számára. A (8) preambulumbekendés többek között megengedi, hogy a GDPR egyes elemeinek tagállami jogba történő implementálását a könnyebb érthetőség érdekében. Az Infotv.-t módosító 2018. évi XXXVIII. törvény⁸⁶ keretében a magyar jogalkotó ezt a lehetőséget használta ki, amikor egyebek mellett átemelte a GDPR fogalomkészletét az Infotv.-be.

II. fejezet

Az információs önrendelkezési jog érvényesülése az általános adatvédelmi rendelet alapján

Az Előszóban már utaltam rá, hogy egy az uniós adatvédelmi reformcsomag keretében megalkotott új jogalkotási termékek meghatározó szerepet töltenek be a jelenleg hatályos szabályozásban. A GDPR hatálybalépésével döntő mértékben egységesült az adatvédelmi szabályozás az Unión belül. A gyakorlati tapasztalatok levonására természetesen évek múltán lesz lehetőség, hiszen szükséges, hogy kialakuljon egy egységes jogalkalmazási gyakorlat, viszont ennek ellenére szükséges a friss jogalkotási termékek vizsgálata és - ahol szükséges - az értékelése. Az elkövetkező fejezetben az információs önrendelkezési jog érvényesülését fogom megvizsgálni a GDPR által biztosított környezetben. Ily módon az érintett személyekre fókuszálva fogom megvizsgálni az általános adatvédelmi rendeletet.

4. A Nemzeti Adatvédelmi és Információszabadság Hatóság, valamint az uniós Adatvédelmi Testület

A GDPR hatályba lépése döntő változásokat hozott az adatvédelemhez való jog biztosításához kapcsolódó intézményrendszer viszonylatában is. Az adatvédelemhez való jog érvényesülése tekintetében kiemelt jelentőséggel bír Hazánk esetében a Nemzeti Adatvédelmi és Információszabadság Hatóság (a továbbiakban: NAIH), valamint az Európai Unió tagállamainak nemzeti hatóságait összefogó, és az adatvédelmi tárgyú jogalkotási aktusokkal kapcsolatos jogértelmezési tevékenységet végző Adatvédelmi Testület (a továbbiakban: Testület). Jogalkalmazó és jogértelmező tevékenységük következtében megkerülhetetlen jelentőséggel rendelkeznek.

4.1. Az Adatvédelmi Testület

Az általános adatvédelmi rendelet sokkal mélyebb változásokat eredményezett az uniós szintű adatvédelmi intézményrendszer tekintetében, mint a tagállami felügyeleti hatóságok esetében. A GDPR hatálybalépésével létrejött az Adatvédelmi Testület, amely az Irányelv által felállított 29. cikk szerinti Adatvédelmi Munkacsoport (a továbbiakban: Munkacsoport) helyébe lépett. A Testület létrehozása részben párhuzamba vonható a NAIH megszervezésével, mind hatásában, mind a jogalkotói megfontolás szempontjából. A következőkben a szervezeti keretek mellett a feladat- és hatáskört, valamint az ezek biztosításához kapcsolódó eljárásrendet fogom ismertetni.

4.2.1. Az Adatvédelmi Testület intézménye

Az Adatvédelmi Testület szervezeti áttekintése során számomra a legfőbb szempontot a függetlenség

⁸³ A közvetlen hatály megállapításában nagy szerepe volt az 1963-as van Gend en Loos döntésnek [ECLI:EU:C:1963:1]. A döntés nyomán kialakult egy feltételrendszer, amely teljesítése esetén megállapítható a közvetlen hatály. Ezek a feltételek, hogy kellően világos legyen, valamint feltétel nélküli szabály legyen (az érvényesülése és végrehajtása ne függjön további feltételtől).

⁸⁴ ECLI:EU:C:1978:17 (Fratelli Zerbone Snc v Amministrazione delle finanze dello Stato)

⁸⁵ ECLI:EU:C:1973:101 (Fratelli Variola S.p.A. v Amministrazione italiana delle Finanze)

⁸⁶ Az információs önrendelkezési jogról és az információszabadságról szóló 2011. évi CXII. törvénynek az Európai Unió adatvédelmi reformjával összefüggő módosításáról, valamint más kapcsolódó törvények módosításáról szóló 2018. évi XXXVIII. törvény

vizsgálata képezte. A GDPR által megkonstruált Testület egy a tagállamok egy - meghatározott - felügyeleti hatóságának vezetőjéből és az európai adatvédelmi biztosból - vagy azok képviselőiből - álló független uniós szerv.⁸⁷ A Rendelet 69. cikke rögzíti, hogy a Testület feladatainak ellátása, illetve hatásköreinek gyakorlása során függetlenül jár el, továbbá ezek ellátása során utasítást nem kérhet, és nem is fogadhat el. Fontos kiemelni, hogy az Adatvédelmi Testület a Munkacsoporttal szemben önálló jogi személyiséggel rendelkezik, így az Európai Unió Bírósága előtt támadható (*alperesi legitimitáció*). A Bizottság eredeti jogalkotási javaslatában még egy uniós ügynökséges kívánt létrehozni, viszont ez az elképzelés hamar elvetésre került.⁸⁸ A függetlenséget tovább erősíti, hogy Munkacsoporttal szemben a Testület elnökét 5 éves időtartamra választják.⁸⁹

Az Irányelvhez képest változások következtek be a Testület összetételében. A tagállamok által kijelölt felügyelő hatóság vagy hatóságok képviselői mellett a Munkacsoport tagjai voltak a közösségi intézmények és szervek nevében létrehozott hatóságok képviselői is, amely alanyi kör a Testület tekintetében már nem szerepel. További változás, hogy a Bizottság által kijelölt képviselő helyébe az európai adatvédelmi biztos lépett. A megelőző szabályozásban érvényesülő jelentős bizottsági jelenlét enyhülését eredményezte a GDPR. A jelenlegi szabályozás értelmében is a bizottság által kijelölt képviselő részt vehet a Testület eljárásain, viszont szavazati joggal már nem rendelkezik.⁹⁰ Az európai adatvédelmi biztos kizárólag az uniós intézményekre, szervekre, hivatalokra és ügynökségekre alkalmazandó azon elveket és szabályokat érintő döntések tekintetében rendelkezik szavazati joggal.⁹¹ Az Európai Unióval szoros kapcsolatban álló országok adatvédelmi hatóságainak képviselői megfigyelőként ugyan részt vehetnek a Testület munkájában, de ez a status kizárólag a GDPR 70. cikke szerinti feladatokkal kapcsolatos eljárásokra korlátozódik.⁹²

Speciális alanyi kört képez az Európai Gazdasági Térség tagállamai közül Izland, Norvégia és Liechtenstein, amelyek nemzeti hatóságainak képviselői kvázi tagjai a Testületnek, viszont a döntéshozatalban szavazati joggal nem rendelkeznek, ellenben a meghozott döntések az ezen államok hatóságait is kötik.⁹³ Ugyan járulékos jogosítványokkal - nevezetesen a döntés kialakításában való közreműködésben - a fenti három állam is rendelkezik, viszont meglátásom szerint ez nem pótolja a szavazati jog hiányát. Hasonlóan, hogy a cégjog sem engedi a *societas leoninat*, jelen helyzetben sem elvárható egy olyan döntésnek való alávetés, amelynek meghozatalában az érintett nem vehet részt. Mindezekből következően mindenképpen szükséges lenne a három hivatkozott állam helyzetének revíziója.

A Testület mellett működő Titkárságot a korábbiaktól Bizottság helyett az európai adatvédelmi biztos biztosítja.⁹⁴ A GDPR által a Testületre ruházott feladatok ellátásában közreműködő alkalmazottak kizárólag a Testület elnökének utasításai alapján végzik a feladataikat,⁹⁵ ezzel kettős függelmi viszonyt állva. Az újonnan megalkotott függelmi rendszer ugyan előrelépést jelent még nem teljesen megfelelő. Annak ellenére, hogy az Európai Unió nem állam - a föderális állam koncepcióját a 2005-ös népszavazások elvetették - viszont sok tekintetben hasonlóan funkcionál, mint egy állam. Ebből következően meg kell felelnie a *Montesquieu* által a *Törvények szelleméről* c. munkájában meghatározott hatalmi ágak megosztásának. Célszerű lenne, egy teljesen elkülönült Titkárság létrehozása, amely minden tekintetben független a végrehajtó hatalmat megtestesítő Bizottságtól. Ennek biztosítását szolgálhatná az Európai Parlament és a Tanács által rendezett költségvetés.

4.1.2. Az Adatvédelmi Testület feladat- és hatásköre

A Testület feladat- és hatáskörével kapcsolatban a legfontosabb annak a körülménynek a kiemelése, hogy

⁸⁷ GDPR 68. cikk (3) bekezdés

⁸⁸ HIJMANS 2016. 149. In.: Péterfalvi, 2018. 329.

⁸⁹ Irányelv 29. cikk (4) bekezdés és a GDPR 73. cikk (2) bekezdés

⁹⁰ GDPR 68. cikk (5) bekezdés

⁹¹ GDPR 68. cikk (6) bekezdés

⁹² PÉTERFALVI, 2018. 332.

⁹³ PÉTERFALVI, 2018. 333.

⁹⁴ Irányelv 29. cikk (5) bekezdés és a GDPR 75. cikk (1) bekezdés

⁹⁵ GDPR 75. cikk (2)-(3) bekezdések

az európai jogalkotó mindenképpen meg kívánta erősíteni az adatkezelés ellenőrzését végző hatóságok jogosítványait. A GDPR hatálybalépése nem járt hatáskörrelvonással, mivel az Irányelv által rögzített tanácsadó szerepköre a továbbiakban is megmaradt. A Testület tanácsadásával elősegíti a Bizottság munkáját az adatvédelmi tárgyú jogalkotási aktusok előkészítése során, továbbá támogatja a nemzeti hatóságok közötti együttműködést. Szükséges azonban megállapítani, hogy a tanácsadó szerep továbbra is *soft law* eszköznek számít.

A GDPR egyik jelentős novuma, hogy a Testület *strict law* jogkörrel is felruházta az adatvédelemhez való jog Európai Unión belüli egységes érvényre jutása érdekében, amelynek a Testület az *egységességi mechanizmus* keretében tesz eleget. A Testület az egységességi mechanizmuson belül *véleményeket* fogad el, valamint *vitarendezési-* és *sürgősségi* eljárásokat folytat le. Fontos megemlíteni, hogy az egységességi mechanizmus során hozott döntések kötelezőek a tagállami hatóságokra nézve.⁹⁶

Vélemény kiadásának két lehetséges esete merülhet fel. Egyrészt abban az esetben, ha egy általános érvényű vagy egynél több tagállamban hatással bíró ügy megvizsgálása azért szükséges, mert az illetékes felügyeleti hatóság, nem megfelelően járt el. A vélemény kibocsátásának másik esete, ha illetékes felügyeleti hatóság a Testülethez fordul az adatvédelmi hatásvizsgálat követelményének, magatartási kódex tervezetének, tanúsító szervezet akkreditációjának jóváhagyásának, általános adatvédelmi kikötések, illetve szerződéses garanciák megfelelőségének, valamint kötelező erejű vállalati szabályok megfelelőségének vizsgálata érdekében.⁹⁷ A Testület véleményelfogadási eljárása hasonlatos a Kúria jogegységi eljárásával, viszont fontos eltérés, hogy a Testület kizárólag olyan kérdésben bocsáthat ki véleményt, amelyben azt még nem tette, a korábbi véleményeihez a Testület kötve van.⁹⁸

A vitarendezési eljárás célja szintén az egységes jogalkalmazás megteremtése. A felügyeleti hatóságok eljárása során előfordulhat, hogy egymástól eltérő jogértelmezésre jutnak. A GDPR egyik fő célkitűzése az uniós szinten megvalósuló egységes jogalkalmazás megteremtése, amely alapvető követelménye a jogbiztonság és a szabad belső piaci kereskedelem biztosítottságának. A vitarendezési eljárás során a Testület kötelező erejű döntést hoz az eltérő álláspontot képviselő felek tekintetében. Péterfalvi írásában kifejti, hogy a Testület által meghozható kötelező erejű döntés átfogó jellegére vonatkozóan még nem született iránymutatás, nem eldöntött kérdés, hogy a Testület kötve van-e a felek álláspontjához, vagy kialakíthat-e egy sajátot.⁹⁹ Véleményem szerint az utóbbi megoldás a követendő, hiszen egyrészt előfordulhat olyan eset, hogy az eltérő álláspontot képviselő felügyeleti hatóságok mindegyike hibás álláspontot vall, másrészt a Testület főszabály szerint kétharmados többséggel¹⁰⁰ dönt a vitarendezés tekintetében, így az eljárás eredménye orientálónan hat a többi tagállami hatóságra is.

A sürgősségi eljárás olyan kivételes helyzetek feloldására szolgál, amelyek esetében az érintettek jogainak és szabadságainak védelme érdekében sürgős fellépésre van szükség. Az ily módon meghozott intézkedések csak ideiglenes jellegűek, a jogalkotó három hónapban maximalizálja az érvényesülésüket.¹⁰¹

4.1.3. A Munkacsoport iránymutatásai

Már említésre került, hogy az általános adatvédelmi rendelet hatályon kívül helyezte az Irányelvet és ezzel együtt a Munkacsoportot is. Ez természetesen érinti az adatvédelmi szabályozás szempontjából kiemelt jelentőséggel bíró munkacsoporti véleményeket és iránymutatásokat is. Ugyanakkor a hatályon kívül helyezés nem érinti az ezen vélemények és iránymutatások által kifejtett joghatásokat. A GDPR 94. cikk (2) bekezdés *expressis verbis* kimondja, hogy a hatályon kívül helyezett irányelvre történő hivatkozásokat az általános adatvédelmi rendeletre történő hivatkozásnak-, a Munkacsoportra történő hivatkozást pedig az Európai Adatvédelmi Testületre történő hivatkozásnak kell tekinteni.¹⁰²

⁹⁶ PÉTERFALVI, 2018. 338.

⁹⁷ GDPR 64. cikk (1) és (2) bekezdések

⁹⁸ GDPR 64. cikk (3) bekezdés

⁹⁹ PÉTERFALVI, 2018. 342.

¹⁰⁰ GDPR 65. cikk (2) bekezdés

¹⁰¹ GDPR 66. cikk

¹⁰² Ilyen megoldással élt a magyar jogalkotó is az Alaptörvény hatályba léptetése kapcsán a régi Alkotmány nyomán meghozott alkotmánybírói határozatok tekintetében.

Az információs önrendelkezési jog érvényesülésének bemutatása során kiemelt jelentőséggel bírnak az Adatvédelmi Testület - és az azt megelőző Munkacsoport - jogértelmező iránymutatásai, véleményei és ajánlásai. A hivatkozott állásfoglalások hozzájárulnak az uniós jogalkotási aktusok - és közvetve az ezekre épülő tagállami jogszabályok - rendelkezéseinek értelmezéséhez és tartalmuk pontosításához.

4.2. A Nemzeti Adatvédelmi és Információszabadság Hatóság

Az Alaptörvény VI. cikk (4) bekezdése rögzíti, hogy „a személyes adatok védelméhez és a közérdekű adatok megismeréséhez való jog érvényesülését sarkalatos törvénnyel létrehozott, független hatóság ellenőrzi.” Az Alaptörvény rendelkezése értelmében az Infotv. NAIH-ra vonatkozó rendelkezései sarkalatos jogszabálynak minősülnek, ily módon erősítve a Hatóság jogi státusát. A Hatóság teljes mértékben független, csak a törvényeknek van alárendelve, feladatkörében nem utasítható, valamint a feladatát más szervektől elkülönülten, befolyásolástól mentesen látja el. A Hatóság számára feladatot csak törvény állapíthat meg.¹⁰³ A NAIH függetlenségét tovább erősíti, hogy szemben az alapvető jogok biztosától tisztségét kilenc éves időtartamra nyeri el, ennél kizárólag az Állami Számvevőszék elnökét választják meg hosszabb időszakokra.¹⁰⁴ A tagállami hatóságok vezetőinek személyes függetlensége nem kerül részletesebb kifejtésre, a tanulmánynak nem célja ennek a bemutatása.

Az Alaptörvény hatályba lépését megelőzően az állampolgári jogok országgyűlési biztosáról szóló törvény¹⁰⁵ által megkonstruált szakombudsmani rendszer keretében, de egységes hivatallal látták el az alapvető jogok - és ezen belül a személyes adatok védelméhez való jog - védelmét. Az Alaptörvény paradigmaváltása következtében az adatvédelemért felelős ombudsman nagyobb önállóságot nyert és immár, mint autonóm államigazgatási szerv látja el a feladatait. Fontos eltérés, hogy míg az alapvető jogok biztosának *soft law* eszközök - ajánlás, kezdeményezés, javaslatétel, Alkotmánybírósághoz fordulás, meghatározott perbe való beavatkozás stb. - állnak a rendelkezésére, addig a NAIH rendelkezik hatósági jogkörrel is. Ily módon olyan különböző eljárásokat folytathat le, mint az adatvédelmi hatósági eljárás, a titokfelügyeleti hatósági eljárás, az adatkezelési engedélyezési eljárás, et cetera.

A GDPR rendelkezései értelmében a „természetes személyek alapvető jogainak és szabadságainak a személyes adataik kezelése tekintetében történő védelme, valamint a személyes adatok Unión belüli szabad áramlásának megkönnyítése érdekében minden tagállam előírja, hogy e rendelet alkalmazásának ellenőrzéséért egy vagy több független közhatalmi szerv (felügyeleti hatóság) felel.”¹⁰⁶ Hazánk viszonylatában a GDPR által meghatározott hatósági feladat- és hatáskört a Magyarország joghatósága alá tartozó jogviszonyok tekintetében a NAIH gyakorolja.¹⁰⁷ Továbbá a NAIH - más szervekkel vagy személyekkel együttműködve - *képviseli Magyarországot* az Európai Unió közös adatvédelmi felügyelő testületeiben.¹⁰⁸ Az általános adatvédelmi rendelet az Irányelvhez képest nem hozott változást a NAIH jogállásában, döntően inkább az eljárását érinteti.

A NAIH-nak mint felügyelő hatóságnak a legfontosabb feladata az adatvédelmi tárgyú jogszabályok betartatása. Az általános adatvédelmi rendelet az 57-58. cikkeiben példálózó jelleggel határozza meg a felügyeleti hatóságok feladat- és hatásköreit. A feladatok részletes ismertetését mellőzve két körülményt szeretnék kiemelni. Egyrészt a GDPR erősíti a tagállami hatóságok egymás közötti, valamint a tagállami hatóságok és a Testület közötti együttműködést. Ennek az egyik megjelenési formája a Testület kapcsán már kifejtett véleményalkotási esetek, valamint például a Testület által lefolytatott vitarendezési eljárás. A másik, hogy hasonlóan a Testület által végzett tanácsadáshoz, a tagállami felügyeleti hatóságom is támogatják a nemzeti szintű adatvédelmi tárgyú jogszabályok megalkotását.¹⁰⁹ Ezzel szakmai alapot képezve a tagállami jogalkotásnak.

A GDPR hatására erősödés figyelhető meg a személyes adatok védelméhez való jog tekintetében. Az egyes nemzeti hatóságok is átvették ezt a szemléletmódot és igyekeznek többletintézkedésekkel, ajánlásokkal

¹⁰³ Infotv. 38. § (5) bekezdés

¹⁰⁴ Infotv. 40. § (3) bekezdés

¹⁰⁵ 1993. évi LIX. törvény

¹⁰⁶ GDPR 51. cikk (1) bekezdése

¹⁰⁷ Infotv. 38. § (2a) bekezdés

¹⁰⁸ Infotv. 38. § (4) bekezdés e) pont

¹⁰⁹ GDPR 57. cikk (1) bekezdés c) pont

elősegíteni az adatvédelemhez való jog biztosítottóságát. Jó példaként szolgál a Romániában létrehozott felügyeleti szerv, a Személyes Adatok Feldolgozását Felügyelő Országos Hatóság (Autoritatea Națională de Supraveghere a Prelucrării Datelor cu Caracter Personal), amely annak ellenére ajánlja az adatvédelmi tisztviselők kijelölését a 250 embernél kevesebb főt foglalkoztató magánvállalkozások számára, hogy a GDPR értelmében ez nem lenne kötelező.¹¹⁰

5. Az információs önrendelkezési jog biztosítottósága

A GDPR szabályanyaga sokkal bővebb, mint a korábban már ismertetett Irányelv. A cikkek számát alapul véve megközelítőleg a háromszorosa, terjedelmét tekintve a több mint négyszerese. A GDPR jelentős része technikai kérdéseket rendez, többek között az adatkezelő tevékenységének szabályozását, a tevékenységével kapcsolatos követelményeket, viszont ennek bemutatása nem célja jelen tanulmánynak. Szem előtt tartva a korábbiakban meghatározott célokat, részletesebb vizsgálatot az érintett személyekhez leginkább kapcsolódó szabályanyagot, az információs önrendelkezési jog érvényesülését - és a kapcsolódó kérdéseket - kívánom bemutatni.

5.1. A személyes adat

A személyes adat fogalmi körének meghatározása az adatvédelmi tárgyú szabályozás *conditio sine qua non*-ja, az említett terminus nélkül értelmezhetetlen a rá épülő szabályozás. Az általános adatvédelmi rendelet meghatározása szerint a személyes adat nem más, mint „azonosított vagy azonosítható természetes személyre („érintett”) vonatkozó bármely információ”.¹¹¹ Péterfalvi megállapítása szerint a GDPR a fogalomkészletben lényeges változást nem hozott, inkább finomított a definíciókon és némileg egyszerűsítette némelyiket. Összegző megfogalmazásra törekedett többek között a személyes adat fogalmának meghatározása esetében is.¹¹² A GDPR-ban rögzített fogalom megegyezik az Irányelvben meghatározottal,¹¹³ a GDPR ugyanakkor mégis előrelépést jelent. Egyrészt már az értelmező rendelkezések között meghatározza a személyes adatok különleges kategóriáit, ezzel szüntette meg az *ex lex* állapotot. A másik, hogy a GDPR főszabály szerint tiltja a különleges adatok kezelését¹¹⁴ - természetesen kivételekkel -, míg az Irányelv¹¹⁵ a tagállamok diszkrecionális döntésére bízta, hogy megtiltják-e. A magyar jogalkotó az Irányelv szabályozásán túlmutatóan már 2012-ben - az új adatvédelmi törvény elfogadásakor - az értelmező rendelkezések közé emelte és meghatározott szenzitív adatokat, valamint meghatározta a bűnügyi személyes adat fogalmát is, viszont ezt az adatvédelmi reform keretében a Bűnügyi irányelvhez kellett igazítani.

A személyes adat egyes fogalmi elemeinek értelmezését az Adatvédelmi Munkacsoport a személyes adat fogalmáról szóló 4/2007. véleményében (a továbbiakban WP 136) fejtette ki.¹¹⁶ A Munkacsoport négy konjunktív elemet különít el egymástól; amelyek a „bármilyen információ”, a „vonatkozó”, az „azonosított vagy azonosítható” és a „természetes személy”. A négy feltétel szoros logikai egységet alkot, viszont célszerű részben külön tárgyalni őket.

A természetes személy tekintetében a kiindulópont az érintett emberi mivolta. A GDPR nem differenciál uniós- és nem uniós polgárok közötti személyes adatkezelés tekintetében,¹¹⁷ ugyanis az adatvédelmet, mint alapvető emberi jogot valamennyi természetes személy számára biztosítani rendeli. A természetes személyt, mint jogalanyt viszont alaposabban meg kell vizsgálni. A GDPR elvi élel mondja ki, hogy a hatálya nem terjed ki a jogi személyekkel kapcsolatos adatkezelésre,¹¹⁸ ide nem értve azt az esetkört, amikor a jogi személy, mint adatkezelő, vagy adatfeldolgozó szerepel. A természetes személyek

¹¹⁰ FRIED Noémi Lujza: Az adatvédelem európai útvesztőjében In: Várad, 2018. (17. évf.) 6. sz. 58.

¹¹¹ GDPR 4. cikk 1. pont

¹¹² PÉTERFALVI, 2018. 65.

¹¹³ Irányelv 2. cikk a) pont

¹¹⁴ GDPR 9. cikk (1) bekezdés

¹¹⁵ Irányelv 8. cikk (1) bekezdés

¹¹⁶ A GDPR 94. cikke ugyan hatályon kívül helyezte az Irányelvet, viszont a (2) bekezdés rendelkezése értelmében „a természetes személyeknek a személyes adatok feldolgozása tekintetében való védelmével foglalkozó munkacsoportra történő hivatkozást az e rendelet által létrehozott Európai Adatvédelmi Testületre történő hivatkozásnak kell tekinteni.”

¹¹⁷ GDPR (2) és (14) preambulumbekendések

¹¹⁸ GDPR (14) preambulumbekendés, valamint 1. cikk (1) bekezdés és 4. cikk 1. pont

tekintetében a jogalanyiságra kell röviden kitérni. A természetes személyek jogalanyisága általános, egyenlő, teljes és feltétlen, viszont ez a tényhelyzet a már megszületett és élő természetes személyek esetében igaz. Az emberről, mint jogalanyról az élve születés és a biológiai halál közötti időtartamban lehet beszélni. A megfogant méhmagzat még nem jogalany, az esetében az élve születés feltétele szükséges a jogalannyá váláshoz.¹¹⁹ Hasonló a probléma a már elhunyt személyek tekintetében is, akik már nem számítanak jogalanyoknak. A GDPR *expressis verbis* ki is jelenti, hogy a rendeletet nem kell alkalmazni az elhunyt személyekkel kapcsolatos adatkezelésre, viszont lehetőséget biztosít a tagállamoknak a védelem kiterjesztésére.¹²⁰ Fontos megemlíteni, hogy az érintett személyi körök nem maradnak jogvédelem nélkül. Az elhunytak tekintetében felmerülhet a Ptk.-ban rögzített kegyeleti jog a szabályozás kiterjesztésének hiányában.¹²¹ A méhmagzatok tekintetében pedig a Munkacsoport fejtette ki a véleményében, hogy a magzat személyes adatai kapcsolatba hozhatók az anyag egészségügyi személyes adataival, ezáltal közvetetten kiterjed rájuk a GDPR által garantált védelem.¹²²

Az érintett természetes személynek *azonosítottnak vagy azonosíthatónak* kell lennie. A GDPR értelmező rendelkezései alapján „*azonosítható az a természetes személy, aki közvetlen vagy közvetett módon, különösen valamely azonosító, például név, szám, helymeghatározó adat, online azonosító vagy a természetes személy testi, fiziológiai, genetikai, szellemi, gazdasági, kulturális vagy szociális azonosságára vonatkozó egy vagy több tényező alapján azonosítható*”.¹²³ Az általános adatvédelmi rendelet Preambuluma az azonosíthatóság tekintetében az észszerűséget állítja zsinórmértéknek. Az észszerűségnek való megfelelés tekintetében olyan objektív körülményekre kell figyelemmel lenni, mint az azonosítás költsége, a ráfordított időmennyiség, valamint a rendelkezésre álló technológia.¹²⁴ Továbbá megkülönböztethető közvetlen és közvetett azonosíthatóság. A Munkacsoport véleménye alapján közvetlen azonosíthatóságot tesz lehetővé az érintett személy neve, valamint az ehhez kapcsolódó - a beazonosítást pontosító - járulékos információk, többek között a lakcím, születési hely és idő. A közvetett azonosíthatóság esetében egyedi kombinációk jelenségéről lehet beszélni. A közvetett azonosíthatóság esetében a rendelkezésre álló információk alapján elsősorban nem lehetséges egy konkrét természetes személy elkülönítése, viszont az információkból levont következtetések megfelelő feldolgozással alkalmasság tehető az érintett beazonosításra.¹²⁵ Adott esetben egy internet felhasználó által folytatott keresések alapján is azonosíthatóvá válik az érintett személy.¹²⁶

Az *információ* lényegében bármire kiterjedhet, a jogalkotói értelmezés meglehetősen bőven határozza meg a lehetséges eseteit. A WP 136. sz. vélemény alapján a kérdéses információ *jellege* alapján lehet objektív (vércsoport), vagy adott esetben szubjektív (az érintett pozitív megítélése) is. *Tartalmát* tekintve valamennyi információt tartalmazó adatra kiterjedhet (az orvos által kiállított ismeretlen betegre vonatkozó vény is).¹²⁷ Az információ bármilyen *formában* rögzítésre kerülhet, a jogalkotó nem követel meg konkrét adathordozási módot.¹²⁸ Az absztrakt meghatározás univerzálissá teszi a szabályozást a permanensen változó technológia mellett. Sőt mindezeket túlmenően az sem elvárta az információval szemben, hogy valós legyen, ennek az az indoka, hogy az érintett számára biztosított a hozzáférés és a kijavítás joga.¹²⁹ Az egyedüli követelmény, a szintén fogalmi elemként támasztott vonatkozás vagyis, hogy valamilyen módon kapcsolódnia kell a korábbiakban részletezett azonosított vagy azonosítható természetes személyhez.

Az utolsó fogalmi elem az információ és a természetes személy közötti *kapcsolat*. Az információ érintett személyre vonatkozása abban az esetben valósul meg, amennyiben közöttük adekvát kapcsolat áll fenn. A Munkacsoport három lehetséges esetkört különített el. Tartalom elemként történő szereplés esetén az

¹¹⁹ 64/1991. (XII. 17.) AB határozat

¹²⁰ GDPR (27) preambulumbekzdés

¹²¹ Ptk. 2:50. §

¹²² WP 136.

¹²³ GDPR 4. cikk 1. pont második fordulat

¹²⁴ GDPR (26) preambulumbekzdés

¹²⁵ WP 136.

¹²⁶ ECLI:EU:C:2019:15 (Commission nationale de l'informatique et des libertés (CNIL) v Google LLC)

¹²⁷ Különös esetkört jelentenek a biometrikus, amelyek a konkrét, tényszerű nációk mellett magukba foglalják az azok alapján levonható megállapításokat is.

¹²⁸ GDPR (15) preambulumbekzdés

¹²⁹ WP 136.

érintettre vonatkozó információt az adatkezelésre tekintet nélkül adják meg, míg a cél elem esetében valamilyen elérendő cél elérése érdekében. A harmadik esetkör az eredmény elem, amelynek az a specialitása, hogy esetében sem a tartalom, sem a cél nem állapítható meg, viszont az információ feldolgozása kihatással lehet az érintettre.¹³⁰

5.2. Az adatkezeléshez kapcsolódó alapelvek

A személyes adatok kezelésére vonatkozóan a GDPR alapvető elvi tételeket határoz meg, amelyek magas absztrakciós szintet képviselnek. Ezen alapelvek egymással korrelatív viszonyban állnak, így együttesen képezik azt a zsinórmértéket, jogalkotói elvárást, amellyel összhangban kell állnia a ráépülő jogi normáknak. Az általános adatvédelmi rendelet tulajdonképpen az adatvédelmi szabályozás kódexének tekinthető, mint *lex generalis*, a szabályanyagán alapulnak az egyes speciális uniós adatkezelési jogalkotási aktusok és tagállami jogszabályok is. A kódex jellegből következően a GDPR alapelveinek valamennyi személyes adatkezelés tárgyú jogszabálynak meg kell felelnie. Az alapelveknek elsődlegesen hézagpótló szerepe van, a Preambulum és az Adatvédelmi Testület értelmező rendelkezéseinek hiányában hivatottak támpontot adni a jogalkalmazóknak. A tagállamok eltérő alapelv-értelmezéséből¹³¹ adódó különbségeket a Munkacsoport WP 203.-as véleménye hivatott mérsékelni. A következőkben az adatvédelmi alapelvek kerülnek rövid ismertetésre, kiemelt figyelmet szentelve a problémaközpontú megközelítésnek, valamint érdemes röviden kitérni a hazai szabályozásra is. Az alapelvek közül kiemelkedik a célhoz kötöttség, és a jogszerűség, amelyek a többi elv levezetésének is alapjául szolgálnak, így ezek bemutatása részletesebben történik.

A *célhoz kötöttség* alapelve¹³² Péterfalvi szerint *primus inter pares* az alapelvek között, előfeltétele a többi alapelv érvényesülésének és az adatkezelés megkezdésének.¹³³ Jóri megállapítja, hogy a célhoz kötöttség elve olyan egyszerre alkotmányos- és a GDPR-ban lefektetett követelmény, amelynek az adatkezelések teljes folyamatában érvényesülnie kell.¹³⁴ Az alkotmányos követelmény tekintetében az Alkotmánybíróság egymást követő határozataiban állapította meg a korlátozhatóság követelményét. A személyes adatok védelméhez való jog korlátozhatósága tekintetében a kiindulópont a korábbiakban már hivatkozott „személyi szám határozat”. Az korlátozásának kibontására viszont csak az 46/1995. (VI. 30.) AB határozatban került sor, ez alapján „a személyes adatok védelméhez való jog, mint alapvető jog korlátozásának meg kell felelnie az alkotmányos követelményeknek. Ez azt jelenti, hogy az információs önrendelkezési jogot [...] mint alapjogot csak elkerülhetetlen esetben lehet alkotmányosan korlátozni, akkor ha a korlátozás elkerülhetetlenül szükséges és az a korlátozással elérni kívánt célhoz képest arányos.” A megengedhetőség tekintetében lényeges kiemelni a 65/2002. (XII. 3.) AB határozatot, amelyben az Alkotmánybíróság „az Alkotmány [...] az alapjogi teszt szükségességi elemét tovább konkretizálta, s az adatkezelés célhoz kötöttségét állította követelményként.” Péterfalvi kifejti, hogy a célhoz kötöttség lényegi tartalma az egyértelmű és egyben jogszerű cél megválasztása, valamint ezt követően a személyes adatok céllal, célokkal összeegyeztethető kezelése.¹³⁵ A GDPR tartalmaz egy bővítő rendelkezést, amely a közérdekű archiválás céljából, tudományos és történelmi kutatási célból vagy statisztikai célból történő további adatkezelést a céllal összeegyeztethetőnek tekinti.¹³⁶

A *jogszerűség, tisztességes eljárás és átláthatóság* alapelve¹³⁷ összetett kritériumrendszert állít fel. A jogszerűség a GDPR értelmezése szerint abban az esetben valósul meg, ha az adatkezelés az érintett hozzájárulásán alapul, vagy egyéb jogszabályi alappal rendelkezik.¹³⁸ Az említett jogszabály lehet a GDPR-tól eltérő norma, adott esetben tagállami jogszabály is. Az uniós jogalkotás ezzel részleges jogalkotási szabadságot biztosít a tagállamoknak, saját jogalkotásukkal jogalapot teremtve az adatkezelésnek. A magyar jogalkotó az Infotv.-ban a véleménynyilvánítás szabadsága tekintetében történő személyes adatkezelést jogszerűnek

¹³⁰ WP 136.

¹³¹ PÉTERFALVI, 2018. 95.

¹³² GDPR 5. cikk (1) bekezdés b) pont

¹³³ PÉTERFALVI, 2018. 96.

¹³⁴ JÓRI, 2018. 96.

¹³⁵ PÉTERFALVI, 2018. 98.

¹³⁶ GDPR 5. cikk (1) bekezdés b) pont második fordulat

¹³⁷ GDPR 5. cikk (1) bekezdés a) pont

¹³⁸ GDPR (40) preambulumbekkezdés

tekinti.¹³⁹ A NAIH ugyanakkor a korábbi adatvédelmi biztosok gyakorlatára is építve a jogalkotóval ellentétes álláspontot képvisel. „*A Hatóság álláspontja szerint közterületen lebet aláírásokat gyűjteni. Aláírásgyűjtés céljából tilos az állampolgárokat személyesen, otthonaikban felkeresni. Ellenkező esetben a pártok tevékenysége az érintettek zaklatásának minősülne, ami súlyosan sértené a polgárok magánszféráját és a tisztességes adatkezelés követelményét.*”¹⁴⁰ Véleményem szerint bár kedvező az állampolgárok közéleti részvétele az államügyek előmenetele szempontjából, ennek ellenére tiszteletben kell tartani az egyének passzív véleménynyilvánítási szabadságát, azaz a hallgatás jogát. A véleménynyilvánítás szabadságának, mint első generációs emberi jognak korlátai vannak ugyan, de tevőleges állami szerepvállalást nem igényel a biztosítása. Továbbá a fenti jogszabályhely visszaélésre adhat alapot, amelynek keretében „*az adatkezelőke lakcím szerinti bontásban listázzák a polgárokat és esetleg úgynevezett „negatív listákat” állítanak össze azokról, akik nem kívánnak részt venni egy kezdeményezésben.*”¹⁴¹ Álláspontom szerint célszerű lenne a hivatkozott jogszabályhely eliminálása. A tisztességesség és az átláthatóság a jogszerűségnél már gyakorlatibb kérdés. Az adatkezelés annyiban minősül tisztességesnek, amennyiben az érintett előzetesen teljes körű tájékoztatást kap az adatkezelőtől. Az átláthatóság tulajdonképpen a tisztességesség biztosítékául szolgál, nevezetesen megköveteli, hogy „*a személyes adatok kezelésével összefüggő tájékoztatás, illetve kommunikáció könnyen hozzáférhető és közérthető legyen, valamint hogy azt világosan és egyszerű nyelvezettel fogalmazzák meg.*”¹⁴² Viszont a GDPR ezen rendelkezése nem egy határozott jogintézmény, így a tartalmát tekintve pontosan nem determinálható.

Az *adattakarékosság elve*,¹⁴³ valamint a *korlátozott tárolhatóság elve*¹⁴⁴ szorosan kapcsolódik a célhoz kötöttség alapelvehez, tartalmát tovább részletezi. A GDPR Preambuluma alapján „*az adatok körét [...] a célhoz szükséges minimumra kell korlátozni. Ehhez pedig biztosítani kell különösen azt, hogy a személyes adatok tárolása a lehető legrövidebb időtartamra korlátozódjon. Személyes adatok csak abban az esetben kezelhetők, ha az adatkezelés célját egyéb eszközzel és egyszerű módon nem lehetséges elérni.*”¹⁴⁵ Az adattakarékosság tekintetében kettős követelménynek kell teljesülnie. Egyrészt csak abban az esetben megengedett az érintett személyes adatainak kezelése, amennyiben az a cél eléréséhez szükséges, másrészt a cél eléréséhez feltétlenül szükséges adatokra kell korlátozódnia az adatkezelésnek.

A *pontosság elve*¹⁴⁶ nem jelent mást, mint azt, hogy a személyes adatok rögzítése során kiemelt figyelmet kell fordítani a kellően precíz adatrögzítésre. A személyes adatok pontatlan rögzítése jelentős hátrányt okozhat többek között a személyazonosító adatok esetében.¹⁴⁷ Péterfalvi értekezése szerint az adatok pontossága nem törvényszerűen jelenti a rögzített személyes adatok objektív pontosságát, hanem sokkal inkább az adatkezelés céljának fényében kell jól megválasztott, releváns személyes adatoknak lenniük. A személyes adatok pontosságának követelményénél vissza kell utalni a Munkacsoport WP 136. sz. véleményére, amelyben meghatározásra került, hogy a személyes adatnak nem fogalmi eleme az, hogy valós legyen. Véleményem szerint az megfelelő személyes adat kérdésének két eltérő szabályozását az indokolja, hogy a személyes adat fogalma kiterjed a jogvédelmi megközelítésre is, míg a pontosság elvének GDPR általi rögzítése azért szükséges, mert - a kezelt személyes adatok esetében - az érintett és az adatkezelő között fennálló jogviszony megköveteli a naprakész adatokat. A pontosság elvéből vezethető le az érintett törléshez és helyesbítéshez való joga.

Az *integritás és bizalmas jelleg elve*¹⁴⁸ korábban nem szerepelt elvként a szabályozásban, az adatbiztonság elve csak követelményként került rögzítésre.¹⁴⁹ A személyes adatokat olyan módon kell kezelni, hogy

¹³⁹ Infotv. 4.§ (5) bekezdés

¹⁴⁰ A Nemzeti Adatvédelmi és Információszabadság Hatóság közleménye a pártok által tervezett aláírásgyűjtésekről, Budapest, 2013. március 19.

¹⁴¹ NAIH közlemény, 2013.

¹⁴² GDPR (39) preambulumbekkezdés

¹⁴³ GDPR 5. cikk (1) bekezdés c) pont

¹⁴⁴ GDPR 5. cikk (1) bekezdés e) pont

¹⁴⁵ GDPR (39) preambulumbekkezdés

¹⁴⁶ GDPR 5. cikk (1) bekezdés d) pont

¹⁴⁷ RÉVÉSZ Balázs – SOMOGYVÁRI Katalin: *Az információszabadság jelentése, tartalma* In: PÉTERFALVI Attila (szerk.): *Adatvédelem és információszabadság a mindennapokban*, Hvg-Orac Lap- és Könyvkiadó Kft., Budapest, 2012. 180-182.

¹⁴⁸ GDPR 5. cikk (1) bekezdés f) pont

¹⁴⁹ PÉTERFALVI, 2018. 106.

megakadályozásra kerüljön a személyes adatok jogosulatlan kezelése, az azokhoz való jogosulatlan hozzáférés. Az adatkezelőnek az adatkezelés körülményeinek átfogó vizsgálata alapján a kockázat mértékének megfelelő szintű adatbiztonságot garantálnia.¹⁵⁰

Az *elszámoltathatóság elve*¹⁵¹ egy többletgarancia a személyes adatok kezelése vonatkozásában. Az alapelv lényegi magva röviden úgy foglалható össze, hogy az adatkezelőnek képesnek kell lennie arra, hogy megfelelően igazolja a jogszabályi rendelkezéseknek megfelelő adatkezelési tevékenységét. Továbbá a felügyeleti hatóságokkal együtt kell működnie a vele szemben lefolytatott vizsgálat során. Az adatkezelő együttműködési kötelezettsége a vizsgálat sikeres lefolytatását akadályozó tevékenységek mellőzésén túl aktív cselekvést vár el az adatkezelőtől.¹⁵²

Az információs önrendelkezési jog, mint nevesített személyiségi jog esetében az adatvédelemhez való jog természete című részben már kifejtésre került, hogy nem abszolút érvényesülést kívánó jog, és *közérdekből korlátozható*. Ily módon a személyes adatok védelmével kapcsolatban megfogalmazott alapelvek sem korlátlanul érvényesülő előírások. A GDPR rendelkezéseinek közérdek általi lerontása tekintetében két hazai példát emelnék ki a joggyakorlatból. Az első eset a törvényszékek cégbíróságai által vezetett *cégnyilvántartás*, amely a gazdaság rentábilis működése érdekében közhitelesen tartalmazza a nyilvántartott jogi személyekhez kapcsolódó meghatározott természetes személyi kör személyes adatait.¹⁵³ A másik eset az egészségügyi személyes adatok, mint különleges adatok egészségügyi intézmények általi nyilvántartása, ahol a járványügyi szempontok érdekében kezelik az *egészségügyi dokumentációk, valamint a zárójelentések* által tartalmazott személyes adatokat.¹⁵⁴ Mind a két esetben sérül a pontosság és az adattakarékosság elve, viszont az elérendő cél meghaladja az alapelvek sérülését.

5.3. Az adatkezelés jogalapja

A személyes adatok jogszerű kezelésének alapvető feltétele, hogy az adatkezelő megfelelő joggal rendelkezzék. Fontos mindazonáltal kiemelni, hogy a - megfelelő - jogalap megléte esetén sem feltétlenül válik jogszerűvé az adatkezelés. A jogalapon túl az adatkezeléssel kapcsolatban megfogalmazott alapelvek, adatkezelői kötelezettségek, valamint az adatkezelés célján való túlterjeszkedés mind a jogszerűtlen adatkezelés megvalósulását eredményezik. A jogalapok két csoportra oszthatók, egyrészt az érintett személy jóváhagyásán alapuló, másrészt a jogalkotók által meghatározott, az érintett jóváhagyását nem igénylő jogalapokra.

Az érintett jóváhagyását nem igénylő csoport esetében érvényesül az adatvédelmi szabályozás partikuláris jellege. A GDPR felhatalmazása alapján az Infotv. kiegészíti az adatkezelés jogalapjait, többek között a tarvényi felhatalmazáson alapuló önkormányzati rendeletekkel. Az Infotv. kiegészül továbbá a bünyügyi irányelvől implementált jogalapokkal. A GDPR által meghatározott érintetti jóváhagyást nem igénylő jogalapok közé tartozik többek között a természetes személy létfontosságú érdekeinek védelme miatt szükséges, vagy az adatkezelőre vonatkozó jogi kötelezettség teljesítéséhez szükséges adatkezelés is. Az érintett jóváhagyását nem igénylő jogalapok további bemutatása viszont nem célja a tanulmánynak. Az érintett jóváhagyásának megnyilvánulása két módon történhet, egyrészt az érintett által adott hozzájárulással, másrészt meghatározott szerződés teljesítéséhez szükséges adatkezeléssel. Az adatkezelés jogalapjainak többsége tekintetében előre meghatározott objektív körülmények teljesülése esetén lehetővé teszi a legitim adatkezelést, viszont a hozzájárulás, mint - kiegészítő jelentőségű - jogalap tekintetében az uniós jogalkotó egy további aktív akaratnyilatkozatot követel meg. Garanciális szabály, hogy ha az adatkezelés hozzájáruláson alapul, az adatkezelőnek képesnek kell lennie annak igazolására, hogy az érintett személyes adatainak kezeléséhez hozzájárult. Továbbá fontos kiemelni, hogy az általános adatvédelmi rendelet felhatalmazza a tagállamokat a Rendelet szabályainak végrehajtása értelmében való további jogalapok meghatározására. Többek között az Infotv. szabályozza a különleges személyes adatok kezelését, amelynek egyik esetekén a törvénnyel kihirdetett nemzetközi szerződés végrehajtásához feltétlenül szükséges és azzal arányos, vagy azt az Alaptörvényben biztosított alapvető jog érvényesítése.

¹⁵⁰ GDPR 32. cikk (1) bekezdés

¹⁵¹ GDPR 5. cikk (2) bekezdés

¹⁵² PÉTERFALVI, 2018. 108-109.

¹⁵³ 2006. évi V. törvény

¹⁵⁴ 1997. évi CLIV. törvény

A GDPR meghatározása szerint az érintett hozzájárulása nem más, mint „az érintett akaratának önkéntes, konkrét és megfelelő tájékoztatáson alapuló és egyértelmű kinyilvánítása, amellyel az érintett nyilatkozat vagy a megerősítést félreérthetetlenül kifejező cselekedet útján jelzi, hogy beleegyezését adja az őt érintő személyes adatok kezeléséhez”.¹⁵⁵ A definíció négy konjunktív feltétel érvényesülését követeli meg a hozzájárulás megadottnak minősítéséhez, ezek az *önkéntesség*, a *konkrétság*, a *megfelelő tájékoztatáson alapultság*, és az *egyértelmű kinyilvánítás*.¹⁵⁶ A 29. cikk szerinti Munkacsoport több döntésében is foglalkozott a hozzájárulás elemeivel.

5.3.1. A hozzájárulás önkéntessége

A Munkacsoport állásfoglalásai alapján az *önkéntesség* nem más, mint egy teljes belátási képességgel rendelkező személy kényszermentes, valódi választási lehetőségen alapuló rendelkezése.¹⁵⁷ A tényleges választási lehetőség fennállása túlmutat a szerződés megkötésének szabad elhatározásán. A Munkacsoport által képviselt álláspont megköveteli, hogy konkrétan a hozzájárulás tekintetében kell fennállnia a szabad döntési lehetőségnek. Amennyiben az adatkezelés egyszerre több célt is szolgál, akkor a hozzájárulást az összes adatkezelési célra vonatkozóan meg kell adni. Nem tekinthető önkéntesnek a hozzájárulás, ha az érintett kizárólag összességében járulhat hozzá a kezelni kívánt személyes adatok feldolgozásához.¹⁵⁸ Az általános várakozásokkal ellentétben viszont több ponton sérülhet az önkéntesség kritériuma, és ennek megfelelően sokkal inkább kisegítő jellegűvé válik a hozzájárulás, mint legitim jogalap. Nem áll fenn tényleges választási lehetőség abban az esetben, ha az egyedi hozzájárulás visszavonását követően tovább folytatják az adatfeldolgozást egy másik jogalap alapján.¹⁵⁹ Az előbbi értelmezésnek megfelelően a hozzájárulás *ultima ratio* jellegű, csak akkor lehet az adatkezelés legitim jogalapja, amennyiben nincs lehetőség más alternatív körülményekre hivatkozni. Az előbbieket levezethetőek a *jogszerűség*, *tisztes eljárás* és *átláthatóság* alapelveiből is.

Az önkéntességgel kapcsolatban további problémákat eredményez, amennyiben a felek nem egyenlő pozícióban állnak, hanem a hozzájárulást adó lényegesen kiszolgáltatottabb. Abban az esetben, ha a szerződés nem tárgyalható részében található a hozzájárulás, akkor nem elégíti ki az önkéntesség követelményét. Ezen a ponton felmerülhet, hogy a hozzájárulás megadását magukba foglaló általános szerződési feltételek is jogsértőnek minősülnek. Az esetükben viszont belép egy másik jogalap, a szerződés teljesítéséhez szükséges adatkezelés, amely legitimálja az adatkezelést. Továbbá a munkáltatók fele történő hozzájárulás esetében is kétséges az önkéntesség a munkaviszony speciális jellegéből következően. Nem lesz önkéntes a hozzájárulás, ha a konkrét munkakörben történő foglalkoztatás folytatásához szükséges a hozzájárulás. Ilyen eset a már betöltött pozíció folytatásához szükséges fényképes igazolótartalmak elkészítése, ennek hiányában pedig más munkakör betöltése. Ezekben az esetekben az önkéntességet az tudja megteremteni, ha joghátrány nélkül lehetősége van a munkavállalónak arra, hogy más alternatív lehetőséget válasszon.

5.3.2. A hozzájárulás konkrétsága

A hozzájárulás tekintetében megfogalmazott konkrétság annak biztosítását célozza, hogy a felhasználó bizonyos mértékben rendelkezzen az adatok felett, az érintett számára pedig biztosítható legyen bizonyos mértékű átláthatóság.¹⁶⁰ A konkrétság megkövetelése a célhoz kötöttség alapelveiből vezethető le. A korábbiakban már kifejtésre került, hogy a célhoz kötöttség *primus inter pares* az alapelvek között, így érvényesülése még a jogalapot is megelőzi. A konkrétság tekintetében Péterfalvi kifejti, hogy meg kell határozni az az adatkezelés pontos és egyértelmű célját, továbbá a személyes adatokat csak abból a célból lehet felhasználni, amelyről az érintettet tájékoztatták, és amelyhez az érintett hozzájárult.¹⁶¹

A konkrétság nagyfokú pontosságot követel meg az adatkezelőtől, hiszen tételes lebontásban kell szerepeltetnie a kezelni kívántszemélyes adatokat, továbbá szelektációs lehetőséget kell biztosítania az

¹⁵⁵ GDPR 4. cikk 11. pont

¹⁵⁶ GDPR (32) preambulumbekzdés

¹⁵⁷ WP259 rev.01.sz. iránymutatás; és WP187.sz. vélemény

¹⁵⁸ GDPR (43) preambulumbekzdés

¹⁵⁹ WP187

¹⁶⁰ WP259 rev.01

¹⁶¹ PÉTERFALVI, 2018. 117-118.

érintett számára.¹⁶² Az érintett jogosult kell, hogy legyen megtagadni egyes személyes adatainak kezelését, nem tehető egységesség a hozzájárulás.

5.3.3. A megfelelő tájékoztatáson alapultság

A GDPR előírásai szerint a hozzájárulás iránti kérelmet elkülönülten, érthető és könnyen hozzáférhető formában, világos és egyszerű nyelvezettel kell előadni.¹⁶³ A GDPR nem határozza meg a teljesítésének formáját és módját, ebből következően az érvényes tájékoztatás különféle képpen közölhető, például szóbeli nyilatkozat, de audioüzenetek formájában is. A tájékoztatás formájának szabadsága mellett ugyanakkor annak tartalma tekintetében már szigorúbb követelményeknek kell eleget tenniük az adatkezelőknek.

A WP259 rev.01 sz. iránymutatás meghatározza az érvényes hozzájárulás szubminimális feltételit. Az érintettet megfelelően tájékoztatni kell az adatkezelő kilétéről; mindegyik olyan adatkezelési művelet céljáról, amelyhez hozzájárulást kérnek; arról, hogy milyen (típusú) adatok gyűjtésére és felhasználására kerül sor; a hozzájárulás visszavonásához való jog létezéséről; adott esetben az adatok automatizált döntéshozatal céljából történő felhasználására vonatkozó tájékoztatás a 22. cikk (2) bekezdése c) pontjának megfelelően; valamint az adattovábbításoknak a megfelelőségi határozat és a 46. cikkben ismertetett megfelelő garanciák hiányából fakadó lehetséges kockázatairól.¹⁶⁴ Az iránymutatás példálózó jelleggel bemutatja a leggyakrabban használt közlési módokat és támpontként szolgál az egyes közlési módok tekintetében a teljes tájékoztatás megteremtéséhez.

Hazánk vonatkozásában a NAIH a 2015/2201/17/H sz. határozatában vizsgálta a hozzájárulás elemeit, különös tekintettel a megfelelő tájékoztatásra. A Hatóság kifejtette, hogy az előzetes megfelelő tájékoztatás alapvető fontosságú az Alaptörvényben rögzített jog gyakorlásához. Az érintett kizárólag a személyét érintő adatkezeléshez tartozó információk teljessége alapján válik képessé az információs önrendelkezési jogának maradéktalan érvényesítésére.

5.3.4. Egyértelmű kinyilvánítás

A hozzájárulás kinyilvánítása tekintetében is több alternatíva áll rendelkezésre. A GDPR nem köti írásbeli alakszerűséghez a hozzáadás megadását, sőt még azt sem várja el, hogy ezt konkrétan kinyilatkoztassa az érintett személy. Az adatkezelés elfogadása történhet olyan magatartás tanúsításával, olyan gyakorlat folytatásával, amely alapján megalapozottan feltehető az érintett beleegyezése. A szabályozás mindazonáltal nem olyan megengedő, ugyanis minden esetben - a kinyilvánítás módjától függetlenül - egy aktív cselekvést feltételez. Egy előre bejelölt négyzet, vagy egy a szerződéstervezet változtathatatlan részébe foglalt kikötés semmilyen esetben sem megfelelő a hozzájárulás megállapításához.¹⁶⁵

6. *Mögöttes személyiség*

Az automatizált adatkezelés nyomán megvalósuló profilalkotás, vagy más szóval a mögöttes személyiség véleményem szerint a legnagyobb kihívást jelentő területe az adatvédelmi szabályozásnak. A korábbiakban említésre került, hogy a GDPR Preambuluma deklarálja azt a célt, hogy az általános gyakorlattól eltérően a jog alakítsa a technológiai változásokat és ne a változások indukálják a jogrendszer módosulását a felmerülő problémák következtében. Pontos következtetések jelenleg még nem vonhatók le, mivel a GDPR viszonylag rövid ideje lépett hatályba, mindazonáltal meglátásom szerint néhány év múlva szükséges lesz a terület problémaorientált revíziója.

6.1. Automatizált döntéshozatal és profilalkotás

Mindenekelőtt fontos kiemelni, hogy az automatizált döntéseket meg lehet hozni profilalkotással vagy anélkül; a profilalkotás történhet automatizált döntéshozatal nélkül. A nem kizárólagosan automatizált

¹⁶² WP259 rev.01

¹⁶³ GDPR 7. cikk (2) bekezdés

¹⁶⁴ WP259 rev.01

¹⁶⁵ GDPR (32) preambulumbekzdés

döntések is magukban foglalhatnak profilalkotást. Azonban a profilalkotás és az automatizált döntéshozatal nem feltétlenül elkülönült tevékenységek.¹⁶⁶ Meg kell említeni, hogy a Munkacsoport WP251rev. sz. iránymutatása alapján a profilalkotás történhet automatizált döntéshozatal nélkül is, viszont ez nem célszerű. A profilalkotás térnyerése a technológiai fejlődéssel jelent meg és szorosan is kapcsolódik hozzá. Végső soron három esetkör különíthető el, az általános profilalkotás; a profilalkotáson alapuló döntéshozatal; és a kizárólag automatizált döntéshozatal. A meghatározások ismertetését követően a GDPR 22. cikk (1) bekezdésében meghatározott kizárólagos automatizált döntéshozatal és az azon alapuló profilalkotás (a továbbiakban: profilalkotás) kerül megvizsgálásra.

Az automatizált döntéshozatal azt jelenti, hogy az érintett személyes adatait különböző elemzőalgoritmusok igénybevételével értékelik ki. Az általános adatvédelmi rendelet értelmező rendelkezései alapján a profilalkotás személyes adatok automatizált kezelésének bármely olyan formája, amelynek során a személyes adatokat valamely természetes személyhez fűződő bizonyos személyes jellemzők értékelésére, különösen a munkahelyi teljesítményhez, gazdasági helyzetéhez, egészségi állapothoz, személyes preferenciákhoz, érdeklődéshez, megbízhatósághoz, viselkedéshez, tartózkodási helyhez vagy mozgáshoz kapcsolódó jellemzők elemzésére vagy előrejelzésére használják.¹⁶⁷ Ily módon a profilalkotás nem más, mint személyes adatok valamilyen formájú automatizált kezelése, amelynek célja egy természetes személy személyes jellemzőinek értékelése.¹⁶⁸ A profilalkotásnál érdemes visszautalni a személyes adat fogalmára. A GDPR által megadott terminus szerint az információ személyes adatnak minősüléséhez elegendő a közvetett azonosíthatóság is. Ily módon a profilalkotás keretében, a természetes személyekre vonatkozó személyes jellemzők bármilyen automatizált személyes adatok kezelése keretében történő kiértékelése nyomán levont következtetések is személyes adatnak fognak minősülni, ezáltal az automatizált adatkezelés során nyert információk tekintetében is alkalmazni kell a hatályos adatvédelmi előírásokat.

A közvetett módon nyert információk alapján egy meglehetősen pontos személyiségrajt alkotható meg. Profilalkotás keretében az érintett közvetett személyes adatai alapján reprodukálható a virtuális térben. A következőkben az előbbiek szerint leírt virtuális személyiség „felhasználása”, és az azzal kapcsolatos aggályok kerülnek ismertetésre.

6.2. Megengedhetőség

Az érintett jogosult arra, hogy ne terjedjen ki rá az olyan, kizárólag automatizált adatkezelésen alapuló döntés hatálya, amely rá nézve joghatással járna vagy őt hasonlóképpen jelentős mértékben érintené.¹⁶⁹ A Munkacsoport az iránymutatásában értelmezi a GDPR hivatkozott szakasz helyét. A szabályozás jellegének meghatározása szempontjából fontos kiemelni, hogy a Munkacsoport iránymutatása alapján az érintett fenntartása a kizárólag automatizált adatkezelésen alapuló döntés tekintetében nem az érintett kifejezett nyilatkozatához kötött.¹⁷⁰ Az adatkezelőt köteles bizonyítani, hogy az érintett kifejezett hozzájárulását adta személyes adatainak automatizált adatkezelés alapján történő kezeléséhez.

A tilalom csak olyan konkrét körülmények között áll fenn, amikor a döntést *kizárólag automatizált adatkezelés* (ideértve a profilalkotást is) alapján hozzák meg, és annak *joghatása vagy egy hasonlóképpen jelentős hatása van* valakire.¹⁷¹ Kizárólagosan automatizált a döntéshozatal, amennyiben emberi közrehatás nélkül történik a személyes adatok feldolgozása, kiértékelése és végül a döntés meghozatala. A Munkacsoport WP251rev.01 sz. iránymutatása alapján nem elegendő a reprezentatív emberi jelenét. Az emberi részvétel abban az esetben valósul meg, ha olyan személy végezni, aki jogkörrel és kompetenciával rendelkezik a döntés megváltoztatására. Az elemzés részeként az összes releváns adatot figyelembe kell venni.¹⁷² A joghatásnak ki kell hatnia az érintett törvényes jogaira, jogállására vagy szerződésen alapuló jogaira. A joghatás mellett említett jelentős hatás nehezebben meghatározható tartalmú, hézagpótló jelentőségű rendelkezés.

¹⁶⁶ WP251rev.01

¹⁶⁷ GDPR 4. cikk 4. pont

¹⁶⁸ WP251rev.01

¹⁶⁹ GDPR 22. cikk (1) bekezdés

¹⁷⁰ WP251rev.01

¹⁷¹ WP251rev.01

¹⁷² WP251rev.01

Lényegében az adatkezelés hatásának kellően nagynak vagy fontosnak kell lennie ahhoz, hogy figyelmet érdemeljen.

A GDPR természetesen ismer még a tilalom elemeinek megléte esetére is kivételes adatkezelési esetköröket, amelyek lehetővé teszik a profilok automatizált döntéshozatalon alapuló meghozatalát. Egyrészt lehetőség van profilalkotásra, amennyiben az *az érintett és az adatkezelő közötti szerződés megkötése vagy teljesítése érdekében szükséges*. Fontos, hogy ebben az esetben a szerződés és a profil megalkotása között alapvető kapcsolat áll fenn. Lehetséges példa egy biztosítási szerződés megkötését megelőző, meghatározott szempontok szerinti értékelése a leendő szerződő félnek. A biztosító kizárólag a lefolytatott elemzés alapján tudja meghozni a döntését, hogy kíván-e egyáltalán szerződést kötni, és ha igen, akkor milyen feltételek mellett. Sor kerülhet a profil megalkotására amennyiben azt *az érintettek jogainak és szabadságainak, valamint jogos érdekeinek védelmét szolgáló uniós vagy tagállami jog teszi lehetővé*. Lehetséges példa csalás és az adókijátszás megelőzése érdekében hozott rendelkezések. Felmerülhetnének a társadalombiztosítás keretében megvalósuló egészségügyi profilok, viszont ezek már különleges adatok alapján kerülnének megalkotásra, amely többletkövetelményekkel jár. Az utolsó lehetséges esetkör *az érintett kifejezett hozzájárulása*. A korábbiakban már részletezésre kerültek a hozzájárulás, mint lehetséges adatkezelési jogalap tekintetében támasztott követelmények, így ismételtelen nem fejteném ki őket. Mindazonáltal fontos ismételtelen leszögezni, hogy a hozzájárulás kiegészítő jellegű, annyiban lesz meg nem tévesztő az adatkezelő tevékenysége, amennyiben nincs más alternatív adatkezelési jogalap.

6.3. Az érintettet megillető jogok fokozott érvényesülésének szükségessége

Már említésre került, hogy a profilok megalkotása során döntően a közvetlen személyes adatok feldolgozása által nyert információkat használják fel. Az áttételes kapcsolat eredményeként viszont lazul a kapcsolat az érintett személy és a hozzá tartozó személyes adat között. Ad absurdum az az élethelyzet is előállhat, hogy az érintettnek nincs is tudomása a hozzá köthető, és azt őt leíró személyes adatok létéről. Ezen okokból következően az érintett személy nehezebben képes érvényesíteni az információs önrendelkezési jogát. Általánosságban is elmondható, hogy az adatkezelők többletpotenciállal rendelkeznek az érintettel szemben, és ezáltal nem teljes mértékben mellérendelt a közöttük fennálló jogviszony. A közvetetten létrejövő személyes adatok tekintetében ez még hatványozottabban igaz, ezért is szükséges egyes érintetti jogok maximális érvényesülése.

A GDPR megköveteli az érintett személy megfelelő *tájékoztatását*.¹⁷³ Az adatkezelőnek könnyen hozzáférhető módon kell tájékoztatást adnia a kizárólag automatizált adatkezelésen alapuló, joghatással vagy hasonlóan jelentős hatással járó automatizált döntéshozatalról, illetve a profilalkotásról. Ebben az esetben az adatkezelőnek közölnie kell az érintettel, hogy ilyen típusú tevékenységet végez, érdemi tájékoztatást kell adnia az adatfeldolgozás során alkalmazott logikáról valamint be kell mutatnia, hogy az ilyen adatkezelés milyen jelentőséggel és milyen várható következményekkel bír az érintettre nézve. Az adatkezelőnek nem kell tételes tájékoztatást adnia - adott esetben ez üzleti titkot is sérthetne egy újfajta algoritmus esetében - viszont meg kell adnia a döntés meghozatalának logikai alapját, illetve az értékelésnél figyelembe általa figyelembe vett szempontokat.¹⁷⁴ Az adatkezelő nem tagadhatja meg a tájékoztatást az adatfeldolgozás összetettségére hivatkozással ugyanis pont a komplexebb műveletek során szükséges a leginkább a megfelelően alapos és érthető tájékoztatás megadása.¹⁷⁵

A *hozzáférési jog* a tájékoztatáshoz való jog mellett hivatott elősegíteni, hogy az érintettek élni tudjanak az őket megillető jogokkal. Minden érintettnek hozzáférési joggal kell rendelkeznie, hogy „megismerje az automatizált adatkezelést, beleértve az alkalmazott logikát, és legalább abban az esetben, amikor az profilalkotásra épül, az ilyen adatkezelés következményeit”.¹⁷⁶

6.4. Szükségtelen profilalkotás és direktmarketing

A profilalkotás megengedhetőségénél már említésre került, hogy szerződés megkötése, illetve teljesítése tekintetében megengedett a személyes adatok automatizált döntéshozatal keretében történő értékelése, és a

¹⁷³ GDPR 13. cikk (2) bekezdés f) pont és 14. cikk (2) bekezdés g) pont

¹⁷⁴ WP251rev.01

¹⁷⁵ GDPR (58) preambulumbekzdés

¹⁷⁶ GDPR 15. cikk (1) bekezdés h) pont

profilalkotás. A biztosítási típusú, vagy hitelszerződések nélkülözhetetlen eleme a profil elkészítése, hiszen e nélkül nem, vagy csak jelentősebb nehézséggel, illetve kockázattal mehetne teljesedésbe az eredeti jogviszony. Viszont nem minden jogviszony keretében szükséges profilt megalkotni, illetve bizonyos körülmények tekintetében a profil megalkotásához mérten szükségtelen mennyiségű személyes adatot gyűjtenek össze és dolgoznak fel.

A nem szükséges profilalkotásnak a hozzájárulás lehet a hozzájárulás a lehetséges jogalapja. A szerződés megkötése, illetve teljesítése, valamint a kellő jogvédelem nem sorolható ebbe a körbe. Megítélésem szerint a hozzájáruláson alapuló profilalkotás szabályozottsága nem kielégítő. Az így megalkotott profilok elsődlegesen az adatkezelők viszonylatában realizálnak hasznot és kiszolgáltatottabbá teszik az érintettet. A korábbiakban meghatározásra kerültek a hozzájárulás elfogadhatóságának kritériumai. Az önkéntesség kizárólag áll fenn, amennyiben tényleges választási lehetőségek közül önkéntesen választhat az érintett. Gyakran felmerül, hogy egyes alkalmazások, vagy oldalak kizárólag a hozzájárulás megadása esetén válnak használhatóvá. Egy képszerkesztő alkalmazás GPS-lokalizációra vonatkozó adatigénylése nem szükséges a szolgáltatás nyújtásához, és túlmutat a nyújtott alapszolgáltatás teljesítésén. A viselkedésalapú hirdetésekhez való hozzájárulás eredményeként az érintett nagy valószínűséggel esik a hirdetés megismerésének lehetőségétől, mivel a gazdasági élet szereplői is egyre inkább célzottan kívánnak hirdetéseket közzétenni. A hozzájárulás elutasításának következményeként az algoritmusok automata döntéshozatal keretében nem irányítanak az érintetthez valamennyi adattartalmat. Továbbá ilyen esetekben sérülnek az adatvédelemmel kapcsolatban meghatározott alapelvek, a jogszerűség, tisztességes eljárás és átláthatóság alapelve, valamint az adattakarékosság elve.

A jogalap megfelelőségén túl a szükségtelenül elkészített profilok további veszélyeket jelenthetnek az érintettre nézve. Az elmúlt években egyre jobban erősödött a *különböző hirdetések* személyre szabottsága. Az éles versenyhelyzet miatt a különböző gyártók termékei között egyre nehezebb objektív módon különbséget tenni, ezért a reklámok a kézzelfogható előnyök helyett a másodlagos előnyökre koncentrálnak. Egyre kevésbé a terméket magát, mint inkább annak hangulatát, az ahhoz kapcsolódó életérzést népszerűsítik.¹⁷⁷ Virányi Péter megfogalmazása szerint: „A modern piac legkelendőbb áruja a boldogság ígérete.”¹⁷⁸ A direktmarketig könnyen versenytorzító hatáshoz vezethet, mivel a kisebb anyagi forrással rendelkező vállalkozások nem képesek olyan mértékben megszólítani a fogyasztókat, mint a piacvezető vállalatok. A kialakuló oligopol piac hátrányosan hathat az érintettekre is.

Az adatkezelők, mint piaci szereplők igyekeznek optimalizálni a gazdasági tevékenységüket ezzel maximalizálni a profitoldalt. Ez adatkezelés tekintetében sincs másként. A nagyobb gazdasági szereplők, amelyek a döntően profilalkotást is végeznek nagy többségében Európán kívül kezelik az érintettek személyes adatait és személyiségprofilját. A GDPR rendelkezései ezen adatok tekintetében is irányadóak, viszont nagyobb sérülékenységet jelent. Viszont ki kell emelni az IBM (International Business Machines) gyakorlatát, amely vállalta, hogy a jövőben nem lesz lehetőség elérni a tárolt adatokat az Európai Unión kívülről.¹⁷⁹

Jelentős kockázattal jár a *munkavállalók helytelen gyakorlata* az adatbiztonság területén. A Kingston kutatása szerint rendkívül elterjedt az USB-k használata a szervezeteknél: szinte minden alkalmazott (84 százalék Magyarországon, 92 százalék az EMEA-országokban) és minden vállalat (94 százalék Magyarországon, 92 százalék az EMEA régióban) használ pendrive-okat. Ráadásul a válaszadók több mint fele vállalati és privát adatokat is tárol ugyanazon az USB kulcsra.¹⁸⁰ Egy megszorítóbb munkahelyi szabályzat sokat lenne képes javítani a kialakult helyzeten.

A *gyermek*ek, mint sérülékeny csoport különösen érintettek a személyes adatokat ért visszaélésekkel szemben. A GDPR szigorúbb rendelkezéseket tartalmaz a gyermekek adatkezelésével kapcsolatban.

¹⁷⁷ <http://mipszi.hu/cikk/091023-reklampszichologia-kialakulasa-fejlodesse> (2019.05.18.)

¹⁷⁸ VIRÁNYI Péter. *Nem igaz, hogy a reklámtól lettem ilyen!* Gondolat Kiadó, Budapest, 2007. 69.

¹⁷⁹ BERKE Barnabásné: *Az európai adatvédelem mellett az IBM* In: Tudományos és műszaki tájékoztatás, 2018. (65. évf.) 2. sz. 140.

¹⁸⁰ BERKE Barnabásné: *A pendrive-használat a céges adatvédelem leggyengébb pontja* In: Tudományos és műszaki tájékoztatás, 2018. (65. évf.) 1. sz. 76.

Főszabály szerint 16 éves kor alatt nem tekinthető megadottnak a gyermek hozzájárulása.¹⁸¹ A témakör terjedelmére való tekintettel a gyermekekkel kapcsolatos adatvédelmi előírásokat egy későbbi tanulmányban fejteném ki.

7. Végkövetkeztetés

A belső piac rentábilis működésének biztosítása megkívánta az adatvédelmi szabályozás egységesítését, valamint az elmúlt évtizedek nyomán végbement technológiai - és társadalmi - változásokból következően is szükségessé vált a 95/46/EK irányelv felülvizsgálata. A jogegységesítésre valóban a rendeleti forma a legalkalmasabb viszont ezzel egy merev, nehezen megváltoztatható keretet szolgál a jelenlegi szabályozásnak, amelyet a Testület jogértelmező tevékenysége hivatott részben feloldani, természetesen a GDPR által meghatározott kereteken belül.

Mindenképpen pozitívként értékelhető a Testület felállítása és jogkörének kibővítése, valamint az Unió végrehajtó hatalmától történő erőteljesebb függetlensége. A Testület keretében megvalósuló kollaboráció hozzájárul az adatvédelemhez való jog fejlesztéséhez és a jogalkalmazás hatékonyságának növeléséhez. tagállami adatvédelmi hatóságok erősödése. A GDPR által bevezetett szankciórendszer további biztosítékát képezi a jogkövető magatartás erősödésének. A GDPR pontosította a különleges személyes adatok körét ezáltal elősegítve a védelem mértékének növelését. Fontos, hogy főszabály szerint a Rendelet tilalmazza a különleges személyes adatok kezelését. Viszont a túlzott megkötések nehezíthetik az egészségügyi dolgozók mindennapi munkáját. A profilalkotás tekintetében észrevehetőek hiányosságok, amelyeket a gazdasági élet szereplői a továbbiakban is képesek lehetnek kihasználni, viszont a Testület tevékenysége képes lehet enyhíteni az uniós jogalkotó ezen a területen tapasztalt mulasztását.

Összességében pozitívan ítélt meg a GDPR, mindenképpen szükséges volt a megalkotása. Az esetleges hiányosságokat pedig a gyakorlat megvizsgálását követően speciális jogalkotási aktusokkal és a Testület jogfejlesztő tevékenységével korrigálni lehet. Nem szabad elfelejteni, hogy a GDPR az általános kereteket határozza meg.

Felhasznált joganyagok

Törvények

1949. évi XX. törvény a Magyar Köztársaság Alkotmánya

1992. évi LXIII. törvény a személyes adatok védelméről és a közérdekű adatok nyilvánosságáról

1993. évi LIX. törvény az állampolgári jogok országgyűlési biztosáról

1997. évi CLIV. törvény az egészségügyről

2002. évi LXI. törvény a Magyar Köztársaság Alkotmányáról szóló 1949. évi XX. törvény módosításáról

2006. évi V. törvény a cégnyilvánosságról, a bírósági cégeljárásról és a végelszámolásról

2009. évi CLV. törvény a minősített adat védelméről

Magyarország Alaptörvénye

2013. évi V. törvény a Polgári Törvénykönyvről

Európai Unió jogalkotási aktusai

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 2000/31/EK Irányelve (2000. június 8.) a belső piacon az információs társadalommal összefüggő szolgáltatások, különösen az elektronikus kereskedelem, egyes jogi vonatkozásairól (Elektronikus kereskedelemről szóló irányelv)

¹⁸¹ GDDPR 8. cikk (1) bekezdés

Debreceni Jogi Műhely 2019. (XVI.) 3-4.
Debreceni Egyetem, Állam- és Jogtudományi Kar, Polgári Jogi Tanszék, Debrecen
(University of Debrecen, Faculty of Law, Department of Civil Law, Debrecen)
DOI 10.24169/DJM/2019/3-4/3

Az Európai Parlament és a Tanács 1049/2001/EK Rendelete (2001. május 30.) az Európai Parlament, a Tanács és a Bizottság dokumentumaihoz való nyilvános hozzáférésről

Az Európai Parlament és a Tanács 45/2001/EK Rendelete (2000. december 18.) a személyes adatok közösségi intézmények és szervek által történő feldolgozása tekintetében az egyének védelméről, valamint az ilyen adatok szabad áramlásáról

Az Európai Parlament és a Tanács 2002/58/EK Irányelve (2002. július 12.) az elektronikus hírközlési ágazatban a személyes adatok kezeléséről, feldolgozásáról és a magánélet védelméről (Elektronikus hírközlési adatvédelmi irányelv)

Az Európai Parlament és a Tanács 2003/98/EK Irányelve (2003. november 17.) a közzféra információinak további felhasználásáról

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)

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

Alkotmánybírósági határozatok

2/1990. (II. 18.) AB határozat

15/1991. (IV. 13.) AB határozat

64/1991. (XII. 17.) AB határozat

46/1995. (VI. 30.) AB határozat

65/2002. (XII. 3.) AB határozat

1053/E/2005. AB határozat

72/2006. (XII.15) AB határozat

22/2016. (XII.5.) AB határozat

Európai Unió Bíróságának döntései

ECLI:EU:C:1963:1 (N. V. Algemene Transport- en Expeditie Onderneming van Gend & Loos v Nederlandse Administratie Der Belastingen)

ECLI:EU:C:1973:101 (Fratelli Variola S.p.A. v Amministrazione italiana delle Finanze)

ECLI:EU:C:1978:17 (Fratelli Zerbone Snc v Amministrazione delle finanze dello Stato)

ECLI:EU:C:2019:15 (Commission nationale de l'informatique et des libertés (CNIL) v Google LLC)

29. cikk szerinti Munkacsoport véleményei, iránymutatásai

4/2007 vélemény a személyes adat fogalmáról (WP 136)

15/2011 vélemény a hozzájárulás meghatározásáról (WP 187)

3/2013 vélemény a célhoz kötöttségről (WP 203)

Iránymutatás az automatizált döntéshozatallal és a profilalkotással kapcsolatban a 2016/679 rendelet alkalmazásához (WP251rev.01)

A 29. cikk szerinti munkacsoport iránymutatása az (EU) 2016/679 rendelet szerinti hozzájárulásról (WP259 rev.01)

Debreceni Jogi Műhely 2019. (XVI.) 3-4.
Debreceni Egyetem, Állam- és Jogtudományi Kar, Polgári Jogi Tanszék, Debrecen
(University of Debrecen, Faculty of Law, Department of Civil Law, Debrecen)
DOI 10.24169/DJM/2019/3-4/3

További jogforrások

Déclaration des droits de l'homme et du citoyen (Az Alkotmányozó Nemzetgyűlés 1789. augusztus 26-án fogadta el.)

Convention for the Protection of Human Rights and Fundamental Freedoms (Róma, 1950. november 4.)

Freedom of Information Act (United States of America, 1966)

International Covenant on Civil and Political Rights (New York, 1966. december 16.)

Convention on Access to Official Documents (Council of Europe, 2008)

Grundgesetz (Német Alaptörvény)

Felhasznált irodalom

PÉTERFALVI Attila – RÉVÉSZ Balázs – BUZÁS Péter: *Magyarázat a GDPR-ról*, Wolters Kluwer Kft., Budapest, 2018.

LAMM Vanda: *Emberi jogi enciklopédia*, Hvg-Orac Lap- és Könyvkiadó Kft., Budapest, 2018.

JÓRI András – SOÓS Andrea Klára – BÁRTFAI Zsolt – HÁRI Anita: *A GDPR magyarázata*, Hvg-Orac Lap- és Könyvkiadó Kft., Budapest, 2018.

Volkszählungsurteil In: TÓTH Zoltán (szerk.): *Informatika-Jog-Közigazgatás – Nemzetközi dokumentumok I.*, InfoFilia, Budapest, 1991.

Grundgesetz In: NÉMETH Lajos (szerk.): *Nemzeti alkotmányok az Európai Unióban*, Wolters Kluwer Kft., Budapest, 2016. 661.

Hilke HIJMANS (2016): *The European Union as a constitutional guardian of internet privacy and data protection* (Phd thesis). University of Amsterdam

https://pure.uva.nl/ws/files/2676507/169421_DEFINITIEF_ZELF_AANGEPAST_full_text_.pdf

BLUTMAN László: *Az Európai Unió joga a gyakorlatban – Második átdolgozott kiadás*, Hvg-Orac Lap- és Könyvkiadó Kft., Budapest, 2013.

RUSZOLY József: *Európai jog- és alkotmánytörténelem*, Pólay Elemér Alapítvány Szeged, 2013.

A Nemzeti Adatvédelmi és Információszabadság Hatóság közleménye a pártok által tervezett aláírásgyűjtésekről, Budapest, 2013. március 19.

KÁRPÁTI József: *A bizalmas adatok kezelése és a magántitok védelme* In: Statisztikai Szemle, 2003. 81. évfolyam 1. szám, 71.

RÉVÉSZ Balázs – SOMOGYVÁRI Katalin: *Az információszabadság jelentése, tartalma* In: PÉTERFALVI Attila (szerk.): *Adatvédelem és információszabadság a mindennapokban*, Hvg-Orac Lap- és Könyvkiadó Kft., Budapest, 2012.

FRIED Noémi Lujza: *Az adatvédelem európai útvesztőjében* In: Várad, 2018. (17. évf.) 6. sz.

Neil WALKER: *Sovereignty in Transition* In: Hart Publishing, 2006.

BERKE Barnabásné: *Az európai adatvédelem mellett az IBM* In: Tudományos és műszaki tájékoztatás, 2018. (65. évf.) 2. sz.

BERKE Barnabásné: *A pendrive-használat a céges adatvédelem leggyengébb pontja* In: Tudományos és műszaki tájékoztatás, 2018. (65. évf.) 1. sz.

VIRÁNYI Péter. *Nem igaz, hogy a reklámtól lettem ilyen!* Gondolat Kiadó, Budapest, 2007.

HABÓK Lilla: *GDPR: 50 millió eurós bírságot kapott a Google* In: hsw.hu (2019.03.12.)

<https://www.hsw.hu/hirek/59894/gdpr-cnil-adatvedelmi-hatosag-google-buntetes.html>

POLGÁR Szilvia: *A reklámpszichológia kialakulása és fejlődése* In: mindennapi pszichológia

Debreceni Jogi Műhely 2019. (XVI.) 3-4.
Debreceni Egyetem, Állam- és Jogtudományi Kar, Polgári Jogi Tanszék, Debrecen
(University of Debrecen, Faculty of Law, Department of Civil Law, Debrecen)
DOI 10.24169/DJM/2019/3-4/3

<http://mipszi.hu/cikk/091023-reklampszichologia-kialakulasa-fejlolese> (2019.05.18.)

BIBLIA, Lukács evangéliuma