

DOKTORI (PhD) ÉRTEKEZÉS

Dr. Tóth Fanni

**Debrecen
2026**

**DEBRECENI EGYETEM
MARTON GÉZA ÁLLAM- ÉS JOGTUDOMÁNYOK DOKTORI
ISKOLA**

**A SZEMÉLYES ADATOK KEZELÉSE AZ EURÓPAI
ADATVÉDELEM, VERSENYJOG ÉS FOGYASZTÓVÉDELEM
METSZÉSPONTJÁBAN**

Készítette:

Dr. Tóth Fanni

Témavezető:

Dr. habil. Hajnal Zsolt PhD

egyetemi docens

A kézirat lezárva: 2026. február 28.

DEBRECEN

2026

NYILATKOZAT

Alulírott, dr. Tóth Fanni, büntetőjogi felelősségem tudatában kijelentem, hogy a Debreceni Egyetem Marton Géza Állam- és Jogtudományi Doktori Iskolában a doktori fokozat megszerzése céljából benyújtott, A személyes adatok kezelése az európai adatvédelem, versenyjog és fogyasztóvédelem metszéspontjában című értekezésem saját önálló munkám, a benne található, másoktól származó gondolatok és adatok eredeti lelőhelyét a hivatkozásokban (lábjegyzetekben), az irodalomjegyzékben, illetve a felhasznált források között hiánytalanul feltüntettem.

Kijelentem, hogy a benyújtott értekezéssel azonos tartalmú értekezést más egyetemen nem nyújtottam be tudományos fokozat megszerzése céljából.

Tudomásul veszem, hogy amennyiben részben vagy egészben sajátomként mutatom be más szellemi alkotását, vagy az értekezésben hamis, esetleg hamisított adatokat használlok, és ezzel a doktori ügyben eljáró testületet vagy személyt megtévesztem vagy tévedésben tartom, a megítélt doktori fokozat visszavonható, a jogerős visszavonó határozatot az egyetem nyilvánosságra hozza.

Debrecen, 2026. február 28.



aláírás

Témavezetői ajánlás

Tóth Fanni

A SZEMÉLYES ADATOK KEZELÉSE AZ EURÓPAI ADATVÉDELEM, VERSENYJOG ÉS FOGYASZTÓVÉDELEM METSZÉSPONTJÁBAN c.

disszertációjának nyilvános vitára bocsátásához

Tisztelt Doktori Tanács!

A hallgató tanulmányai során folyamatosan konzultált, a doktori iskolai kötelezettségeit kiegyensúlyozottan a konzulens és a doktori iskola által meghatározott követelmények szerint teljesítette.

Tanulmányainak kezdetekor a kutatás területeként a személyes adatok védelmére vonatkozó szabályozást, valamint a fogyasztóvédelmi szabályozás metszéspontjait állítottuk. A kutatás középpontjába állított terület azóta rengeteg impulzust kapott, köszönhetően az Európai Unió jogalkotásának, számos alap feltevés igazolódott be, a jogalkotásnak köszönhetően rengeteg alapvetőnek tartott tézis változott meg, és érzékelhetően kialakulni látszott az úgynevezett fogyasztóvédelmi adatjognak nevezhető szabályozási terület, amely az adatvédelmi szabályok és a fogyasztóvédelmi szabályok egy jól körülhatárolható területeként ragadható meg.

A disszertáció központi eleme a személyes adat, valamint a kezelésére vonatkozó szabályozás, amellyel kapcsolatban elsősorban a GDPR és az elektronikus hírközlési adatvédelmi irányelv szabályait elemzi a szerző, majd az adatvédelmen túl a versenyjogi és a fogyasztóvédelmi szempontokat is figyelembe veszi, illetve feltérképezi mindazon jogi aktusokat, amelyek a fogyasztók személyes adatainak a védelmét szerződési jogi vagy éppen online piacokra vonatkozó szabályozási szempontból biztosítják.

A disszertációban a szerző négy kérdéssel foglalkozik:

- Tisztában vannak-e a felhasználók a személyes adataik értékével, gazdasági értéké válásának folyamatával, valamint hogy a GDPR által biztosított átlátható tájékoztatáshoz való jog segíti-e őket tájékozott döntést hozni a személyes adataik kezelésével kapcsolatban, képes-e az információs aszimmetriát ellensúlyozni?
- Milyen mértékben képes a GDPR rendeletjellege és területi hatálya biztosítani az érintettek egységes védelmét az EU-ban, különös tekintettel a fogalomrendszer alkalmazhatóságára, az adatkezelési alapelvek érvényesülésére, az érintetti jogokra és a végrehajtás kérdéseire; valamint megfelelő védelmi szintet biztosít-e az elektronikus hírközlési adatvédelmi irányelv a felhasználók számára?
- A személyes adatok kezelése és a piaci verseny összefüggése alapján a GDPR mely rendelkezései váltak további szigorítást motiváló tényezővé, valamint a platformjogszabályokban testet öltő szigorítások milyen irányban képesek befolyásolni a piaci versenyt?

- Az EU fogyasztóvédelmi eszközrendszere képes-e a fogyasztók – személyes adatokkal kapcsolatos – aszimmetrikus helyzetének kezelésére?

A szerző a releváns szakirodalmat feldolgozva, az alapozó kutatásokat nem elhanyagolva jutott el a dolgozatának központi elemét jelentő fogyasztók személyes adatainak védelmét, felhasználását érintő kérdések tárgyalásához. Jó érzékkel határolta körül a kutatási területét, elemezte a vonatkozó hazai, uniós és külföldi joggyakorlatot, elemezte az egyes szabályozási megoldások előnyeit és hátrányait.

Véleményem szerint Tóth Fanni dolgozatának témája aktuális, a fogyasztóvédelem és adatvédelem metszéspontjaival foglalkozó disszertáció nem született még, a terjedelme, a felhasznált irodalom mennyisége, a szerző által készített szemléltető ábrák alkalmazása mind arra utal, hogy mélyreható kutatással alapozta meg tudományos álláspontjának megfogalmazását.

A munkahelyi vitán elhangzottak figyelembevételével továbbra is úgy gondolom, hogy Tóth Fanni disszertációja, átdolgozott változatában, alkalmas arra, hogy nyilvános vitán mérettesen meg.

Debrecen, 2026. április 23.



Dr. Hajnal Zsolt

egyetemi docens

témavezető

Tartalom

GYAKRAN HIVATKOZOTT JOGSZABÁLYOK ÉS SZERVEZETEK JEGYZÉKE	10
BEVEZETÉS	14
1. Motiváció és témamegjelölés.....	14
2. Alapkérdések, hipotézisek és a disszertáció szerkezeti felépítése	16
3. A kutatás módszerei	22
I. FEJEZET: FOGALMI MEGKÖZELÍTÉSEK ÉS AZ ADATVÉDELEM TÖRTÉNETE ..	24
1. A fogyasztó fogalma	24
1.1. Az átlagfogyasztó és a kiszolgáltató fogyasztó.....	31
1.2. Az átlagfogyasztó a digitális környezetben.....	34
1.3. Összegzés és következtetés	35
2. Az adatvédelmi szabályozás kialakulása és fejlődése.....	36
3. Alapfogalmak.....	45
3.1. Az adatvédelem	45
3.2. A magánélet.....	46
3.3. Az információs önrendelkezési jog	48
3.4. A személyes adat	49
3.4.1. Átnevezítés és anonimizálás	54
3.5. Az adatkezelés, az adatkezelő és az adatfeldolgozó.....	56
4. Az érintett és a fogyasztó	60
5. Összegzés és következtetés.....	62
II. FEJEZET: A SZEMÉLYES ADATOK ÉRTÉKÉNEK JELENTŐSÉGE.....	64
1. A big data és az online platformok.....	65
2. A platformok és a marketingkommunikáció	66
3. Az online platformok adatgyűjtési módszerei.....	67
3.1. A személyes adatok aktív rendelkezésre bocsátása.....	68
3.1.1. A hozzájárulás	68
3.1.2. Tud-e az érintett tájékozott döntést hozni a személyes adatai kezelésével kapcsolatban?	70
3.1.3. Az úgynevezett ingyenes szolgáltatások kérdésköre	75
3.2. A személyes adatok passzív rendelkezésre bocsátása	78
3.2.1. A jogos érdek	78
3.2.2. A felhasználók eszközein elhelyezett cookie-k – az elektronikus hírközlési adatvédelmi irányelv vonatkozó rendelkezései	79
3.2.3. A hazai szabályozás	80

3.3. Következtetésekből származó adatok – a profilalkotás intézménye	80
3.3.1. A profil felhasználása más területeken.....	82
4. A személyre szabott hirdetések veszélyei	84
5. A személyre szabott hirdetések előnyei	84
6. Közgazdasági-pszichológiai kitekintés	85
7. Lehetséges védelmi mechanizmusok	86
7.1. Hozzájárulást vagy díjfizetést megkövetelő modellek.....	88
7.2. Védekezés a szolgáltatás devalválása ellen.....	89
8. Összegzés és következtetés	91
III. FEJEZET: AZ ÉRINTETTEK SZÁMÁRA BIZTOSÍTOTT VÉDELEM SZINTJE A SZEMÉLYES ADATAIK KEZELÉSE TEKINTETÉBEN – A GDPR	93
1. A GDPR és a tagállamok mozgástere	93
2. A GDPR területi hatálya	94
3. A GDPR végrehajtása: a felügyeleti hatóságok	97
3.1. Az egyablakos ügyintézési mechanizmus	97
3.2. A GDPR eljárási rendelete	100
4. Az érintettek jogai a GDPR alapján	102
4.1. Átlátható tájékoztatás és a tájékoztatáshoz való jog	102
4.2. Az érintett hozzáférési joga.....	105
4.3. A helyesbítéshez való jog.....	106
4.4. A törléshez való jog (elfeledtetéshez való jog)	107
4.5. Az adatkezelés korlátozásához való jog.....	109
4.6. Az adathordozhatósághoz való jog.....	110
4.7. A tiltakozáshoz való jog.....	112
4.8. Automatizált döntéshozatal egyedi ügyekben, beleértve a profilalkotást is	114
4.9. A GDPR érintetti jogai és a fogyasztóvédelmi jog összefüggései	118
5. Az adatkezelés alapvető elvei.....	120
5.1. Beépített és alapértelmezett adatvédelem	120
5.2. Az elszámoltathatóság elve	124
6. Az adatvédelmi hatásvizsgálat	125
7. Összegzés és következtetések	128
IV. FEJEZET: AZ ELEKTRONIKUS HÍRKÖZLÉSI ADATVÉDELMI IRÁNYELV ÁLTAL BIZTOSÍTOTT VÉDELEM SZINTJE ÉS AZ UTÓBBI ÉVEK JOGALKOTÁSI JAVASLATAI	131
1. Az elektronikus hírközlési adatvédelmi irányelv és a GDPR	131
2. Szabályozási terv rendelettel.....	134

3. A digitális omnibusz csomag javaslatának vonatkozó rendelkezései	135
4. A digitális omnibusz csomag javaslatának hatása a közvetlen üzletszerzési célú tájékoztatás lehetőségére	138
5. Összegzés és következtetés	140
V. FEJEZET: A SZEMÉLYES ADATOK ÉS AZ ADATVÉDELEM SZEREPE A PIACI VERSENYT ÉRINTŐ PLATFORMJOGSZABÁLYOKBAN	141
1. A GDPR mint fékezőerő?	141
2. A DMA.....	143
2.1. A GDPR és a DMA rendelkezéseinek összevetése a személyes adatok tekintetében	145
3. A Data Act.....	148
3.1. A GDPR és a Data Act rendelkezéseinek összevetése a személyes adatok tekintetében	149
4. Jögesetek az uniós versenyjog és az adatvédelem metszéspontjában	151
4.1. Facebook/WhatsApp ügy	153
4.2. Facebook (Meta Platforms) kontra Bundeskartellamt ügy	154
4.3. Google/Fitbit ügy	160
4.4. A versenyjogi ügyek idővonala.....	161
4.5. A versenyjogi ügyek tapasztalatai	163
5. Összegzés és következtetés	165
VI. FEJEZET: A FOGYASZTÓVÉDELEM ESZKÖZRENDSZERE – A SZEMÉLYES ADATOKKAL ÖSSZEFÜGGÉSBEN	166
1. Adatvédelem, piaci verseny és fogyasztóvédelem, valamint ezek uniós szabályozásának összefonódása.....	166
1.1. Jögesetek az adatvédelem, a versenyjog és a fogyasztóvédelem metszetében	167
2. A fogyasztóvédelmi eszközrendszer a fogyasztók aszimmetrikus helyzetének kezelésére	169
2.1. Kockázatkezelés, átláthatóság, kiskorúak védelme – a DSA a fogyasztók védelmében	170
2.1.1. A DSA által támasztott követelmények	172
2.1.2. A GDPR és a DSA rendelkezéseinek összevetése a személyes adatok tekintetében...	174
2.2. Szerződések szabályozása	178
2.2.1. A UCT-irányelv – a tisztességtelen szerződési feltételekről.....	178
2.2.2. A DCS-irányelv – a személyes adatok mint ellenérték.....	179
2.2.3. A CR-irányelv – tájékoztatási kötelezettség és átláthatóság a távollévők között kötött szerződésekben.....	181
2.3. A UCP-irányelv – a tisztességtelen kereskedelmi gyakorlatok tilalma	183
2.4. Sötét megoldások az online platformok gyakorlatában	186
2.4.1. Sötét megoldások a platformjogszabályokban	191
3. A digitális sérülékenység kezelési lehetőségei.....	194

4. Koherencia vagy széttöredezettség?.....	196
5. Sajátos szabályozási terület születőben – fogyasztóvédelmi adatjog?.....	199
6. Összegzés és a fogyasztóvédelemben rejlő lehetőségek a jövőre vonatkozóan.....	203
VII. FEJEZET: ÖSSZEGZŐ GONDOLATOK, KÖVETKEZTETÉSEK	205
MELLÉKLETEK	218
1. melléklet: A magánélet tipológiája	218
2. melléklet: Érintett és fogyasztó – az online szolgáltatásokkal összefüggésben	218
3. melléklet: A profilalkotás intézménye és a kockázatok a különböző szektorokban	219
4. melléklet: Az adatvédelmi hatásvizsgálat folyamatának lépései	219
5. melléklet: A digitális piacon érintettek helyzete a DMA alkalmazása előtt és után	220
6. melléklet: A fogyasztóközpontú uniós szabályozási logika területei és fejlődése	222
FELHASZNÁLT IRODALOM	223
Szakirodalmi források	223
Európai uniós és nemzetközi jogszabályok.....	233
Magyar jogszabályok	236
EUB-ítéletek.....	237
Egyéb ítéletek.....	238
Versenýügyek.....	238
GVH-ügyek	239
NAIH-dokumentumok	239
A 29. cikk alapján létrehozott munkacsoport és az EDPB dokumentumai.....	239
Európai uniós dokumentumok	241
Egyéb irodalom	244

GYAKRAN HIVATKOZOTT JOGSZABÁLYOK ÉS SZERVEZETEK JEGYZÉKE

EURÓPAI UNIÓS JOGSZABÁLYOK ÉS -JAVASLATOK	
RÖVID NÉV	HIVATALOS NÉV
108. számú egyezmény	Egyezmény az egyének védelméről a személyes adatok gépi felhasználása során
2006/24/EK irányelv	Az Európai Parlament és a Tanács 2006/24/EK irányelve (2006. március 15.) a nyilvánosan elérhető elektronikus hírközlési szolgáltatások nyújtása, illetve a nyilvános hírközlő hálózatok szolgáltatása keretében előállított vagy feldolgozott adatok megőrzéséről és a 2002/58/EK irányelv módosításáról. Hatályos 2006. 05. 03-ig
Adatvédelmi irányelv	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
Általános termékbiztonságról szóló rendelet	Az Európai Parlament és a Tanács (EU) 2023/988 rendelete (2023. május 10.) az általános termékbiztonságról, az 1025/2012/EU európai parlamenti és tanácsi rendelet és az (EU) 2020/1828 európai parlamenti és tanácsi irányelv módosításáról, valamint a 2001/95/EK európai parlamenti és tanácsi irányelv és a 87/357/EGK tanácsi irányelv hatályon kívül helyezéséről
Brüsszel Ia. rendelet	Az Európai Parlament és a Tanács 1215/2012/EU rendelete (2012. december 12.) a polgári és kereskedelmi ügyekben a joghatóságról, valamint a határozatok elismeréséről és végrehajtásáról
Charta	Az Európai Unió alapjogi chartája (2012/C 326/02)
CR-irányelv (Consumer Rights Directive)	Az Európai Parlament és a Tanács 2011. október 25-i 2011/83/EU irányelve a fogyasztók jogairól, a 93/13/EGK tanácsi irányelv és az 1999/44/EK európai parlamenti és tanácsi irányelv módosításáról, valamint a 85/577/EGK tanácsi irányelv és a 97/7/EK európai parlamenti és tanácsi irányelv hatályon kívül helyezéséről
Data Act	Az Európai Parlament és a Tanács (EU) 2023/2854 rendelete (2023. december 13.) a méltányos adathozzáférésre és -felhasználásra vonatkozó harmonizált szabályokról, valamint az (EU) 2017/2394 rendelet és az (EU) 2020/1828 irányelv módosításáról
DCS-irányelv (Digital Content and Services Directive)	Az Európai Parlament és a Tanács (EU) 2019/770 irányelve (2019. május 20.) a digitális tartalom szolgáltatására és digitális szolgáltatások nyújtására irányuló szerződések egyes vonatkozásairól
Digitális omnibusz csomag javaslata	COM(2025) 837 final. Javaslat. Az Európai Parlament és a Tanács rendelete az (EU) 2016/679, az (EU) 2018/1724, az (EU) 2018/1725 és az (EU) 2023/2854 rendelet, valamint a 2002/58/EK, az (EU) 2022/2555 és az (EU) 2022/2557 irányelv digitális jogszabályi keret egyszerűsítése tekintetében történő módosításáról, valamint az (EU) 2018/1807, az (EU) 2019/1150 és

	az (EU) 2022/868 rendelet és az (EU) 2019/1024 irányelv hatályon kívül helyezéséről
DMA (Digital Markets Act)	Az Európai Parlament és a Tanács (EU) 2022/1925 rendelete (2022. szeptember 14.) a digitális ágazat vonatkozásában a versengő és tisztességes piacokról, valamint az (EU) 2019/1937 és az (EU) 2020/1828 irányelv módosításáról
DSA (Digital Services Act)	Az Európai Parlament és a Tanács (EU) 2022/2065 rendelete (2022. október 19.) a digitális szolgáltatások egységes piacáról és a 2000/31/EK irányelv módosításáról
EJEE	Emberi jogok európai egyezménye
EJENY	Emberi jogok egyetemes nyilatkozata
Elektronikus hírközlési adatvédelmi irányelv	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)
E-Privacy rendelet tervezete (2017)	COM(2017) 10 final. 2017/0003 (COD). Javaslat. Az Európai Parlament és a Tanács rendelete az elektronikus hírközlés során a magánélet tiszteletben tartásáról és a személyes adatok védelméről, valamint a 2002/58/EK irányelv hatályon kívül helyezéséről
E-Privacy rendelet tervezete (6087/21)	ST 6087 2021 INIT. Proposal for a Regulation of the European Parliament and of the Council concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications)
EUMSZ	Az Európai Unió működéséről szóló szerződés
EUSZ	Az Európai Unióról szóló szerződés
Fogyasztói hitelmegállapodásokról szóló irányelv	Az Európai Parlament és a Tanács (EU) 2023/2225 irányelve (2023. október 18.) a fogyasztói hitelmegállapodásokról és a 2008/48/EK irányelv hatályon kívül helyezéséről
Fúziós rendelet	A Tanács 139/2004/EK rendelete (2004. január 20.) a vállalkozások közötti összefonódások ellenőrzéséről (az EK összefonódás-ellenőrzési rendelete)
GDPR (General Data Protection Regulation)	Az Európai Parlament és a Tanács (EU) 2016/679 rendelete (2016. április 27.) a természetes személyeknek a személyes adatok kezelése tekintetében történő védelméről és az ilyen adatok szabad áramlásáról, valamint a 95/46/EK irányelv hatályon kívül helyezéséről (általános adatvédelmi rendelet)
GDPR eljárási rendelethe	Az Európai Parlament és a Tanács (EU) 2025/2518 rendelete (2025. november 26.) az (EU) 2016/679 rendelet végrehajtására vonatkozó további eljárási szabályok megállapításáról
Geo-blocking rendelet	Az Európai Parlament és a Tanács (EU) 2018/302 rendelete (2018. február 28.) a belső piacon belül a vevő állampolgársága, lakóhelye vagy letelepedési helye alapján történő indokolatlan területi alapú tartalomkorlátozással és a megkülönböztetés egyéb formáival szembeni fellépésről, valamint a 2006/2004/EK és az (EU) 2017/2394 rendelet, továbbá a 2009/22/EK irányelv módosításáról
Képviselési keresetokról szóló irányelv	Az Európai Parlament és a Tanács (EU) 2020/1828 irányelve (2020. november 25.) a fogyasztók kollektív érdekeinek védelmére irányuló képviselési keresetokról és a 2009/22/EK irányelv hatályon kívül helyezéséről

OECD-irányelvek	OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data (1980). (OECD Irányelvek a magánélet védelméről és a személyes adatok határokon átvitelő áramlásáról)
Omnibusz irányelv	Az Európai Parlament és a Tanács 2019/2161 irányelve (2019. november 27.) a 93/13/EGK tanácsi irányelvnek, valamint a 98/6/EK, a 2005/29/EK és a 2011/83/EU európai parlamenti és tanácsi irányelvnek az uniós fogyasztóvédelmi szabályok hatékonyabb végrehajtása és korszerűsítése tekintetében történő módosításáról
Róma I. rendelet	Az Európai Parlament és a Tanács 593/2008/EK rendelete (2008. június 17.) a szerződéses kötelezettségekre alkalmazandó jogról
Termékfelelősségi irányelv	Az Európai Parlament és a Tanács (EU) 2024/2853 irányelve (2024. október 23.) a hibás termékekért való felelősségről és a 85/374/EGK tanácsi irányelv hatályon kívül helyezéséről
UCP-irányelv (Unfair Commercial Practices Directive)	Az Európai Parlament és a Tanács 2005/29/EK irányelve a belső piacon az üzleti vállalkozások fogyasztókkal szemben folytatott tisztességtelen kereskedelmi gyakorlatairól, valamint a 84/450/EGK tanácsi irányelv, a 97/7/EK, a 98/27/EK és a 2002/65/EK európai parlamenti és tanácsi irányelvek, valamint a 2006/2004/EK európai parlamenti és tanácsi rendelet módosításáról
UCT-irányelv (Unfair Contract Terms Directive)	A Tanács 93/13/EGK irányelve (1993. április 5.) a fogyasztókkal kötött szerződésekben alkalmazott tisztességtelen feltételekről
Utazási csomagokról szóló irányelv	Az Európai Parlament és a Tanács (EU) 2015/2302 irányelve (2015. november 25.) az utazási csomagokról és az utazási szolgáltatás együttesekről, valamint a 2006/2004/EK rendelet és a 2011/83/EU európai parlamenti és tanácsi irányelv módosításáról, továbbá a 90/314/EGK tanácsi irányelv hatályon kívül helyezéséről
MAGYAR JOGSZABÁLYOK	
RÖVID NÉV	HIVATALOS NÉV
45/2014. (II. 26.) kormányrendelet	45/2014. (II. 26.) Korm. rendelet a fogyasztó és a vállalkozás közötti szerződések részletes szabályairól
Fgy. tv.	1997. évi CLV. törvény a fogyasztóvédelemről
Fttv.	2008. évi XLVII. törvény a fogyasztókkal szembeni tisztességtelen kereskedelmi gyakorlat tilalmáról
Grt.	2008. évi XLVIII. törvény a gazdasági reklámtevékenység alapvető feltételeiről és egyes korlátairól
Infotv.	2011. évi CXII. törvény az információs önrendelkezési jogról és az információszabadságról
Ptk.	2013. évi V. törvény a Polgári Törvénykönyvről
Tpvt.	1996. évi LVII. törvény a tisztességtelen piaci magatartás és a versenykorlátozás tilalmáról
SZERVEZETEK	

RÖVID NÉV	HIVATALOS NÉV
AGCM	Autorità Garante della Concorrenza e del Mercato (olasz verseny- és piacfelügyelet)
BEUC (Bureau Européen des Unions de Consommateurs)	European Consumer Organisation (‘Európai Fogyasztói Szervezet’)
Bundeskartellamt	Német versenyhatóság (‘Szövetségi Kartelliroda’)
EDPB	European Data Protection Board (Európai Adatvédelmi Testület)
EJEB	Emberi Jogok Európai Bírósága
EU	Európai Unió
EUB	Európai Unió Bírósága (Court of Justice of the European Union (CJEU))
GVH	Gazdasági Versenyhivatal
NAIH	Nemzeti Adatvédelmi és Információszabadság Hatóság
WP29	Article 29 Data Protection Working Party (29. cikk alapján létrehozott adatvédelmi munkacsoport)

BEVEZETÉS

1. Motiváció és témamegjelölés

A doktori iskolában folytatott tanulmányaim elején ötlött eszembe az a beszélgetés, amely arról szólt, hogy a fővárosi levéltárat az adatvédelmi hatóság¹ megbírságolta, mert személyes adatok kerültek nyilvánosságra – adott levéltári kutatással összefüggésben – egy 1962-es bűnügy kapcsán. Időben egybeesett ez az általános adatvédelmi rendelet, a GDPR² alkalmazásának kezdetével. Ez a két tény együttesen keltette fel érdeklődésemet, és segített meghatározni azt a témakört, amellyel dolgozatomban foglalkozni szeretnék: a személyes adatok szerepe és kezelésük szabályozása az Európai Unióban (a továbbiakban: EU).

A digitális gazdaságban a személyes adatok kulcsszerepet játszanak, általuk nőtt ki az üzleti modell, amely az online platformok és az ökoszisztémák dominanciájához vezetett. A másik oldalon a személyes adataikkal elvileg rendelkező adatalanyok állnak, akik többnyire valamely jogviszony alapján válnak érintetté: munkavállalók, könyvtári tagok, terméket vásárlók vagy szolgáltatást igénybe vevők. Utóbbiak egyúttal fogyasztók is, sőt maga az adatkezelési tájékoztató és tágabb értelemben a GDPR is speciális fogyasztóvédelmi szabályzatnak³ tekinthető. Különösen hangsúlyossá tette az adatvédelem és a fogyasztóvédelem szerepét a technológiai fejlődés rohamos üteme, a platformok révén folyamatosan megjelenő új kihívások, amelyek rámutattak arra, hogy – bár a fogyasztóvédelemnek szerves részét képezi a fogyasztók adatainak védelme – a kettő között bonyolult, komplex a kapcsolat.

Az online platformok adatkezelése nemcsak az egyes érintettekre, felhasználókra gyakorol hatást, hanem a digitális gazdaság többi szereplőjére is, így az üzleti felhasználókra, a harmadik felekre is, ami felvetette az adatgyűjtés és -kezelés szerepének elemzését a piaci versenyt érintő folyamatokban, valamint a bizottsági és hatósági döntésekben, majd szabályozásának szükségességét a versenyjogban. Mindezek elengedhetetlenül megkövetelik az adatvédelem, a fogyasztóvédelem és a versenyjog összehangolt, szabályozási szintű együttműködését. A jogalkotói szándék elmozdulása 2017-től datálható, amikor a Facebook megsértette a fúziós rendeletet, és kétéves felkészülés után, 2019-től a platformok szabályozását

¹ Nemzeti Adatvédelmi és Információszabadság Hatóság (a továbbiakban: NAIH)

² Az Európai Parlament és a Tanács (EU) 2016/679 rendelete (2016. április 27.) a természetes személyeknek a személyes adatok kezelése tekintetében történő védelméről és az ilyen adatok szabad áramlásáról, valamint a 95/46/EK irányelv hatályon kívül helyezéséről (a továbbiakban: GDPR)

³ Wolfgang KERBER: *Competition Law in Context: The Example of its Interplay with Data Protection Law from an Economic Perspective*. *Wirtschaft und Wettbewerb* 2021/7–8. 4. (pdf) https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3890603 (letöltés: 2024. 02. 02.); Verica TRSTENJAK: *GDPR as a New Consumer Protection „Weapon”?* *European Studies – the Review of European law, Economics and Politics* 2024/2. 16. DOI: 10.2478/eustu-2024-0014 (letöltés: 2025. 12. 30.)

célzó jogalkotási eljárások, aktusok sokasága látott napvilágot, példaként említve a digitális piacokról szóló⁴ és a digitális szolgáltatásokról szóló ikerrendeletet⁵ vagy az adatrendeletet.⁶ A megtorpanás éppen a 2025. év elején következett be azzal, hogy kiderült, közel tízéves folyamat sem volt elegendő az új elektronikus hírközlési adatvédelmi jogszabály, az e-Privacy rendelet elfogadására, ezért a javaslatot visszavonták.⁷ Továbbra is rés marad tehát az adatvédelemben. Az említett jogalkotási folyamatokkal szembe kellett néznem választott témám megközelítése során, ami jelentősen felülírta terveimet, és megkövetelte azt, hogy az EU személyes adatokat érintő új jogalkotási aktusaival is foglalkozzam.

Az EU a digitális környezetre vonatkozó jogszabályokat illetően nagyszabású módosításokat tervez, ezért az „egyszerűbb és gyorsabb Európa” céljai jegyében a 2025. év végétől újabb jogalkotási hullám vette kezdetét.⁸ Ennek része a digitális omnibusz csomag javaslata,⁹ melynek szemlélete összefüggésbe hozható az EU kedvezőtlen gazdasági mutatóival¹⁰ és a Draghi-jelentéssel¹¹ is. Mindezek háttérében az a felismerés (is) áll, hogy nem lehet biztosan igennel felelni arra a kérdésre, hogy a GDPR maradéktalanul tudja-e a címében szereplő két cél – a természetes személyek védelme az adatkezelés során és az adatok szabad áramlásának biztosítása – egyensúlyát biztosítani. A közeljövő jogalkotási folyamatait kísérő viták tétje az lesz, hogy az alapjogi védelmet elsődlegesnek tekintő álláspontot felváltja-e az

⁴ Az Európai Parlament és a Tanács (EU) 2022/1925 rendelete (2022. szeptember 14.) a digitális ágazat vonatkozásában a versengő és tisztességes piacokról, valamint az (EU) 2019/1937 és az (EU) 2020/1828 irányelv módosításáról (a továbbiakban: DMA)

⁵ Az Európai Parlament és a Tanács (EU) 2022/2065 rendelete (2022. október 19.) a digitális szolgáltatások egységes piacról és a 2000/31/EK irányelv módosításáról (a továbbiakban: DSA)

⁶ Az Európai Parlament és a Tanács (EU) 2023/2854 rendelete (2023. december 13.) a méltányos adathozzáférésre és -felhasználásra vonatkozó harmonizált szabályokról, valamint az (EU) 2017/2394 rendelet és az (EU) 2020/1828 irányelv módosításáról (a továbbiakban: Data Act)

⁷ COM(2025) 45 final. Mellékletek a következőhöz: A Bizottság közleménye az Európai Parlamentnek, a Tanácsnak, az Európai Gazdasági és Szociális Bizottságnak és a Régiók Bizottságának: A Bizottság 2025. évi munkaprogramja. Strasbourg, 2025. 02. 11. 28.

⁸ COM(2025) 47 final. A Bizottság közleménye az Európai Parlamentnek, a Tanácsnak, az Európai Gazdasági és Szociális Bizottságnak és a Régiók Bizottságának: Egyszerűbb és gyorsabb Európa: Közlemény a végrehajtásról és az egyszerűsítésről. Strasbourg, 2025. 02. 11.

⁹ COM(2025) 837 final. Javaslat. Az Európai Parlament és a Tanács rendelete az (EU) 2016/679, az (EU) 2018/1724, az (EU) 2018/1725 és az (EU) 2023/2854 rendelet, valamint a 2002/58/EK, az (EU) 2022/2555 és az (EU) 2022/2557 irányelv digitális jogszabályi keret egyszerűsítése tekintetében történő módosításáról, valamint az (EU) 2018/1807, az (EU) 2019/1150 és az (EU) 2022/868 rendelet és az (EU) 2019/1024 irányelv hatályon kívül helyezéséről (a továbbiakban: digitális omnibusz csomag javaslata)

¹⁰ A természetes személyek védelme és az adatok szabad áramlásának biztosítása között húzódó arányok (is) szerepet játszanak abban, hogy a globális digitális gazdaságra vonatkozó mutatók szerint az EU az USA és Kína után csak a harmadik helyet tudta megszerezni, és az előrejelzések sem kedvezőbbek az EU számára. EHANGZHOU.GOV.CN: *Digital economy becomes new growth engine for China and other G20 members*. 2024. augusztus 6. https://www.ehangzhou.gov.cn/2024-08/06/c_282384.htm (letöltés: 2024. 11. 05.)

¹¹ *The future of European competitiveness Part A: A competitiveness strategy for Europe*. 2024. szeptember (a továbbiakban: Draghi-jelentés A); *The future of European competitiveness Part B: In-depth analysis and recommendations*. 2024. szeptember (a továbbiakban: Draghi-jelentés B). https://commission.europa.eu/topics/competitiveness/draghi-report_en (letöltés: 2025. 11. 05.)

adatok szabad áramlását segítő, az innovációnak és a versenyképességnek utat nyitó¹² megközelítés, tanulva a digitális nagyhatalmak, az USA és Kína adatkezelési szemléletéből.

Dolgozatom középponti fogalma a személyes adat, valamint a kezelésére vonatkozó szabályozás, elsősorban a GDPR és az elektronikus hírközlési adatvédelmi irányelv¹³ elemzésével, majd a versenyjogi és a fogyasztóvédelmi szempontokat is figyelembe veszem, és megvizsgálom azokat a kapcsolódó jogi aktusokat, amelyek a személyes adatokkal összefüggésben tartalmaznak rendelkezéseket. A dolgozatban az elemzett jogszabályok egymással való kapcsolata szintén hangsúlyos elemként jelenik meg. A jogszabályok vizsgálata megköveteli a joggyakorlattal összevetést, a kapcsolódó jogesetek elemzését, ebben a tekintetben nehézséget jelentett az, hogy a viszonylag új jogszabályokkal kapcsolatban még csak körvonalazódnak ilyenek.

E dolgozat adatvédelmi, platform- és fogyasztóvédelmi jogszabályokat is vizsgál, ezek jogalanyait adott kontextusnak megfelelően nevezem meg, tehát érintettnek, felhasználónak/igénybevevőnek vagy fogyasztónak. Azokban az esetekben, amikor adott szövegrész több jogalanyra együttesen vonatkozik, ott a felhasználó fogalmat részesítem előnyben. Hasonló jellegű problémát vet fel a digitális gazdaságban a szolgáltató megnevezése, amellyel kapcsolatban az előző elv alapján járok el, tehát a vonatkozó jogszabály fogalomhasználatát (adatkezelő, platform stb.) követem, egyéb esetekben a gyűjtőnévi értelmű szolgáltató nevet használom.¹⁴

2. Alapkérdések, hipotézisek és a disszertáció szerkezeti felépítése

A dolgozatban a személyes adatok kezelésének olyan átfogó körképét kívánom bemutatni, amely elvezet a digitális környezetben az adatvédelem, a versenyjog és a fogyasztóvédelem metszéspontjainak feltárásához, a piaci versenyre és a fogyasztókra gyakorolt hatás értelmezéséhez. Egységbe foglalom azokat az európai uniós (a továbbiakban: uniós) jogforrásokat, amelyek az érintettek védelmén őrködnek a személyes adataik kezelésével összefüggésben. Ennek érdekében részletesen elemzem a GDPR-t és az elektronikus hírközlési adatvédelmi irányelvet, valamint ez utóbbihoz kapcsolódva az EU megoldáskereső

¹² Digitális omnibusz csomag javaslata (9) preambulumbekzdés

¹³ 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 (a továbbiakban: elektronikus hírközlési adatvédelmi irányelv)

¹⁴ Gyakran használt fogalom még az adatvezérelt vállalkozás. Meg kell jegyezni, hogy az adatvezérelt vállalat és a platform nem teljesen egynemű kifejezések (előbbi gazdasági kategória, utóbbi jogi fogalom); és nem minden esetben azonos kört fednek le (egy piactér platform, de nem adatvezérelt vállalat; egy adatbróker cég adatvezérelt vállalat, de nem platform), használata abban az esetben indokolt, ha adott vállalat mindkét kategóriába beleillik.

próbálkozásait, azaz röviden érintem az e-Privacy rendelettervezetet,¹⁵ valamint – mivel a szabályozási törekvés fejlődési íve megkívánja – a digitális omnibusz csomag javaslatának cookie-kra vonatkozó rendelkezéseit és azok értékelését beépítem a dolgozatba. A csomagjavaslat több tekintetben érinti a GDPR rendelkezéseit és a versenyjogi jogszabályokat is, a módosítási javaslatokra röviden utalok. Elemzem továbbá az EU platformokkal kapcsolatos legújabb jogalkotási aktusait, valamint a kapcsolódó fogyasztóvédelmi intézkedéseket. Elhatárolódom azonban a mesterséges intelligenciával kapcsolatos jogi szabályozás áttekintésétől.

A dolgozat szerkezeti felépítését tekintve a logika azt kívánja, hogy az alapfogalmak tisztázása után a személyes adatok értékével, értékének jelentőségével foglalkozzam. A személyes adatok gazdasági jelentősége egyrészt összefügg az adatgyűjtés módszereivel, másrészt megalapozza az érintetti jogok bemutatását, valamint az elektronikus hírközlési adatok szerepének és szabályozásának bemutatását. Ezt követően a személyes adatok piaci versenyben betöltött szerepére majd a fogyasztóvédelmi szempontokra koncentrálok. Mivel az adatok mindkét jogterület esetében meghatározók, a versenyjogi és a fogyasztóvédelmi szál is átszövi egymást, mégis indokoltnak tartom külön fejezetben bemutatni ezeket, mert ugyanazt a piaci magatartást más szempontból értékeli és szabályozzák a versenyjogi és a fogyasztóvédelmi jogszabályok.

Az I. fejezet a dolgozat témájának kulcsfogalmait – a személyes adat és a fogyasztó – tekinti át, valamint az ezekhez szorosan tapadó fogalmakat. A fogalmi tisztázás célja az, hogy egyértelmű keretek közé szorítsa a fontos fogalmak jelentését és használatát, ami különösen a további kérdések vizsgálata során nyújt segítséget, valamint hogy láttassa, a két jogterület fogalmi rendszere megállja-e a helyét a digitális környezetben. A fejezethez tartozik a definíciók szerepének gyakorlati szempontú elemzése is a vonatkozó jogesetek alapján, rámutatva ezáltal a jogértelmezési különbségek lehetőségére.

A széttagolt fogyasztóvédelmi eszközrendszerben különösen nagy jelentősége van annak, hogy egységes, stabil fogalmi alapok, de legalább azonos megközelítési szempontok hassanak a koherencia irányában. Fontosnak tartom megvizsgálni azt is, hogy az EU milyen szempontok alapján biztosít differenciált megközelítést a különböző fogyasztói csoportok, így

¹⁵ COM(2017) 10 final. 2017/0003 (COD). Javaslat. Az Európai Parlament és a Tanács rendelete az elektronikus hírközlés során a magánélet tisztteletben tartásáról és a személyes adatok védelméről, valamint a 2002/58/EK irányelv hatályon kívül helyezéséről (a továbbiakban: e-Privacy rendelet tervezete). Utolsó szövegváltozata: ST 6087 2021 INIT. Proposal for a Regulation of the European Parliament and of the Council concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications) (a továbbiakban a lábjegyzetekben: e-Privacy rendelet tervezete (6087/21))

az átlagfogyasztó és a kiszolgáltató fogyasztó számára, valamint hogy a digitális környezetben biztosítottak-e a fogyasztók tényleges védelmének keretei. Ezek mélyreható elemzése rávilágíthat a fogyasztófogalom fejlődési irányára, a várható tendenciákra.

Az adatvédelemmel kapcsolatban mind az érintetti, mind az adatkezelői oldalhoz tartozó fogalmak jelentését felfejtem, valamint a személyes adatnak és fajtáinak definícióit is. A definíciók fogalmi elemeinek feltérképezése és a gyakorlati alkalmazhatóságuk alapján kívánom értékelni az adatvédelem fogalmi apparátusát abból a szempontból, hogy az adekvát-e a modern kor érintettjeinek és fogyasztóinak védelméhez. Nem maradhat el az érintett és a fogyasztó fogalmának alanyi kör szerinti összehasonlítása, a kettő közötti kapcsolódási pontok és különbségek bemutatása sem. Szorosan kötődik mindehhez az adatvédelmi szabályozás történeti bemutatása, amely a kiváltó okokra és a fejlődési irányra koncentrálna azokat a tényezőket veszi számba, amelyek a GDPR megalkotásához vezettek.

Tisztában vannak-e a felhasználók a személyes adataik értékével, gazdasági értéké válásának folyamatával, valamint hogy a GDPR által biztosított átlátható tájékoztatáshoz való jog segíti-e őket tájékozott döntést hozni a személyes adataik kezelésével kapcsolatban, képes-e az információs aszimmetriát ellensúlyozni? – e kérdésekre keresi a választ a II. fejezet. A válaszadáshoz előzetesen a big data, a nagy adatvagyonok forrásait kell látni. A vonatkozó elemzés fontos eleme az adatgyűjtési módszerek, a GDPR szerinti jogalapok, valamint a felhasználó eszközein elhelyezett cookie-k szerepének vizsgálata éppúgy, mint a következtetésekből származó adatok és a profilalkotás értékének feltérképezése. Ezeknek kulcsszerepe van a platformok üzleti modelljeinek működésében és fejlődésében, különösen a személyre szabott hirdetésekkel összefüggésben. Az elemzés által feltárulhat az a folyamat, amelynek során a személyes adatok a profilalkotás által személyre szabott hirdetéssé válva a célzott felhasználók online felületein megjelenhetnek. A tolakodó személyre szabott hirdetések ellen elengedhetetlen a védelmi mechanizmus számbavétele és a hozzájárulást vagy díjfizetést megkövetelő modellek értékelése. A személyes adatok értékének vizsgálata során nem tekinthetünk el a szolgáltatások devalválásának problémáitól sem.

A fogyasztóvédelem szempontjából kulcsfontosságú szerepet játszik a GDPR, hiszen az adatvédelem a fogyasztók jogainak egyik területe, az érintettnek minősülő felhasználók a GDPR alapján rendelkezhetnek a saját személyes adataikkal, amelyeket a piac másik oldala elvileg e rendelet alapján kezel. A GDPR rendelkezései az adatkezelési tájékoztatóban öltönek testet, ami célja szerint az érintetteket, a felhasználókat támogatja a platformokkal szemben fennálló egyensúlyhiány felszámolásában, a személyes adataikra vonatkozó döntések

meghozatalában. Az elemzés kiterjed arra is, hogy az érintettek tájékoztatáshoz való joga és az adatkezelési tájékoztató alkalmas-e az információs aszimmetria kezelésére.

Hipotézisem szerint az érintettek nincsenek tisztában személyes adataik értékével, valamint a GDPR átláthatósági követelményei és az adatkezelési tájékoztató a gyakorlatban nem segíti őket az információs aszimmetria feloldásában.

A III–IV. fejezet azt a kérdést járja körül, hogy milyen mértékben képes a GDPR rendeleti jellege és területi hatálya biztosítani az érintettek egységes védelmét az EU-ban, különös tekintettel a fogalomrendszer alkalmazhatóságára, az adatkezelési alapelvek érvényesülésére, az érintetti jogokra és a végrehajtás kérdéseire; valamint megfelelő védelmi szintet biztosít-e az elektronikus hírközlési adatvédelmi irányelv a felhasználók számára.

E tekintetben először a GDPR-ra összpontosítok (III. fejezet), majd az elektronikus hírközlési adatvédelmi irányelvet vizsgálom, ill. az utóbbihoz kapcsolódóan az utóbbi évek jogszabályjavaslatait is (IV. fejezet). A válaszadáshoz szükséges a GDPR-szabályozás főbb elemeinek, köztük a területi hatálynak, az érintetti jogoknak, az adatkezelési elveknek, a végrehajtásnak és az adatvédelmi hatásvizsgálatnak a mélyreható elemzése. Ezeket a GDPR – adatvédelmi irányelvhez viszonyított – újdonságaival párhuzamosan bontom ki. Az adatvédelmi szabályozás szálai alkalmat adnak fogyasztóvédelmi kitekintésre is, ezáltal előremutatnak e terület eszközeinek irányába is. A cookie-k kezelésére vonatkozóan az elektronikus hírközlési adatvédelmi irányelv és a GDPR kapcsolódási pontjainak értelmezését elengedhetetlennek tartom, emellett a visszavont e-Privacy rendeletjavaslat tervezett cookie-szabályozását, valamint a digitális omnibusz csomag javaslatának idetartozó rendelkezéseit vizsgálom. Megállapítom – a II. fejezetben tárgyalt, a személyes adatok gazdasági értékének jelentőségéhez kapcsolódva – a személyre szabott hirdetésekre vonatkozó uniós szabályozás fejlődési irányát.

Feltételezésem szerint a GDPR rendeleti jellege és területi hatálya alapvetően alkalmas az érintettek egységes védelmét biztosítani az EU-ban, azonban a végrehajtási rendszere, főleg a határokon átnyúló ügyekben, nem hatékony, továbbá fogalomrendszerének értelmezési bizonytalanságai és az érintetti jogok gyakorlati érvényesülésének nehézségei korlátozzák a teljes körű védelem lehetőségét. Az elektronikus hírközlési adatvédelmi irányelv cookie-szabályozása azonban nem biztosítja megfelelően a felhasználók védelmét. A III–IV. fejezet gondolatmenete és a vizsgálati szempontok alapján – a jogszabáylelemzést, -összehasonlítást és a gyakorlati megközelítést lehetővé tévő, kapcsolódó esetjogot segítségül hívva – leszűrhető következtetések várhatóan igazolják a fenti hipotézisemet.

A dolgozat V. fejezete a személyes adatok és az adatvédelem digitális gazdaságban és piaci versenyben betöltött szerepét vizsgálja. Az online platformok adatkezelési gyakorlata miatt, főleg a célzott hirdetésekkel kapcsolatos tevékenységükkel összefüggésben, erőteljesebb védelemre és a végrehajtás megszilárdítására van szükség. Többek között ez vezetett el az EU részéről ahhoz a felismeréshez, hogy további jogszabályi megerősítésre van szükség. A döntéshez hozzájárultak a versenyhatósági és a bizottsági vizsgálatok tapasztalatai, ideértve a nagy ügyekből levont konzekvenciákat mind a tisztességes piaci verseny, mind a felhasználók érdekében a személyes adatok kezelésére vonatkozóan. Mindezek a következő kérdés vizsgálatát kívánják: A személyes adatok kezelése és a piaci verseny összefüggése alapján a GDPR mely rendelkezései váltak további szigorítást motiváló tényezővé, valamint a platformjogszabályokban testet öltő szigorítások milyen irányban képesek befolyásolni a piaci versenyt?

A kérdéskör megválaszolásához elemzem a személyes adatok szerepét és hatását a piaci versenyben, néhány jelentős fúziós és antitröszt ügy folyamatát, ezek következményeit a döntéshozói és jogalkotói szándékra, valamint a tapasztalatok beágyazódását egy új terület, a platformjog¹⁶ szabályozásába. E körben a kapuöröket regulázó DMA-re és az adatmegosztást erőteljesen támogató Data Actre fókuszálok. Számba veszem azokat a konkrét GDPR-rendeleteket, amelyek megizmosodva épültek be az említett, 2019 és 2024 között keletkezett jogalkotási aktusokba, és a személyes adatok felhasználásának piaci versenyt befolyásoló szerepét szabályozzák. E rendelkezések egy része az üzleti felhasználók érdekében a versenypozíciójuk javítását célozza, de ezzel párhuzamosan a fogyasztók lehetőségeit is támogatja, ha ezekkel élni tudnak és akarnak.

Hipotézisem szerint – mivel szoros összefüggés mutatható ki a platformok személyesadat-kezelése és a piaci verseny alakulása között – a platformjogszabályok egyrészt szigorítják a GDPR jogszerű jogalapra vonatkozó rendelkezéseinek alkalmazhatóságát, másrészt megerősítik az érintetti jogok közül azokat, amelyek lehetővé teszik, hogy a személyes adatok ténylegesen beépüljenek a digitális gazdaságba, de egyúttal korlátozva a nagy platformok adatkezelését, és teret adva a piaci versenynek.

A fogyasztók védelmét az EU kezdetben a szerződési feltételek, a kereskedelmi gyakorlatok stb. szabályozásával biztosította. Mivel a digitális környezet és a platformok térnyerése miatt valamely magatartás fogyasztóvédelmi és adatvédelmi szempontból egyaránt releváns lehet, kikristályosodtak olyan csomópontok, amelyek az adatvédelmi rendelkezések

¹⁶ ZÖDI Zsolt: *Az európai platformszabályozás jellegzetességei: Platformjog és felhasználóvédelem*. In *Medias Res* 2022/1. 72. (a továbbiakban: ZÖDI (2022))

megegyeztetését igényelték a fogyasztóvédelmi jogforrásokban is. 2019-től az omnibusz irányelv¹⁷ korszerűsítő törekvései a védelem határait is kiterjesztették, és a meglévő jogszabályokba a személyes adatok kezelésével kapcsolatos rendelkezéseket emeltek be, valamint egy önálló norma is született, a DCS-irányelv.¹⁸ A következő fontos állomást a DSA jelentette, ezt követően egyre erőteljesebbé vált a folyamat, és egyre több jogszabályban – képviseleti keresetekről szóló irányelv,¹⁹ általános termékbiztonságról szóló rendelet,²⁰ fogyasztói hitelmegállapodásokról szóló irányelv,²¹ új termékfelelősségi irányelv²² – kerültek nevesítésre adatvédelmi rendelkezések. Az utóbbiak különösen felhívják a figyelmet arra, hogy az algoritmusok alkalmazásával összefüggő közvetlen vagy közvetett kockázatok a fogyasztók erőteljesebb védelmét kívánják. Mindezekből következően a VI. fejezet arra fókuszál, hogy az EU fogyasztóvédelmi eszközrendszere képes-e a fogyasztók – személyes adatokkal kapcsolatos – aszimmetrikus helyzetének kezelésére.

Az elemzés ennek megfelelően kiterjed a fogyasztóvédelem klasszikus területeinek adatvédelmi rendelkezéseire; másrészt kifejezetten az online közvetítő szolgáltatókra, köztük a platformokra szabott jogi aktus, a DSA vizsgálatára. Valamennyi érintett jogszabállyal kapcsolatban hangsúlyt kap az, hogy a sötét megoldásokra tudnak-e reagálni, és rendelkezéseik értelmezhetők-e a digitális környezetben, adaptálhatók-e arra. A sötét megoldások mellett többek között a személyre szabott hirdetések és a profilalkotás is szabályozást váltott ki több fogyasztóvédelmi jogszabályban. Tekintettel arra, hogy például a GDPR, a UCP-irányelv²³ és a DSA is csak a saját eszközeivel tudja a problémákat kezelni, ez azzal járhat, hogy a

¹⁷ Az Európai Parlament és a Tanács 2019/2161 irányelve (2019. november 27.) a 93/13/EGK tanácsi irányelvnek, valamint a 98/6/EK, a 2005/29/EK és a 2011/83/EU európai parlamenti és tanácsi irányelvnek az uniós fogyasztóvédelmi szabályok hatékonyabb végrehajtása és korszerűsítése tekintetében történő módosításáról (a továbbiakban: omnibusz irányelv)

¹⁸ Az Európai Parlament és a Tanács (EU) 2019/770 irányelve (2019. május 20.) a digitális tartalom szolgáltatására és digitális szolgáltatások nyújtására irányuló szerződések egyes vonatkozásairól (a továbbiakban: DCS-irányelv)

¹⁹ Az Európai Parlament és a Tanács (EU) 2020/1828 irányelve (2020. november 25.) a fogyasztók kollektív érdekeinek védelmére irányuló képviseleti keresetekről és a 2009/22/EK irányelv hatályon kívül helyezéséről (a továbbiakban: képviseleti keresetekről szóló irányelv)

²⁰ Az Európai Parlament és a Tanács (EU) 2023/988 rendelete (2023. május 10.) az általános termékbiztonságról, az 1025/2012/EU európai parlamenti és tanácsi rendelet és az (EU) 2020/1828 európai parlamenti és tanácsi irányelv módosításáról, valamint a 2001/95/EK európai parlamenti és tanácsi irányelv és a 87/357/EGK tanácsi irányelv hatályon kívül helyezéséről (a továbbiakban: általános termékbiztonságról szóló rendelet)

²¹ Az Európai Parlament és a Tanács (EU) 2023/2225 irányelve (2023. október 18.) a fogyasztói hitelmegállapodásokról és a 2008/48/EK irányelv hatályon kívül helyezéséről (a továbbiakban: fogyasztói hitelmegállapodásokról szóló irányelv)

²² Az Európai Parlament és a Tanács (EU) 2024/2853 irányelve (2024. október 23.) a hibás termékekért való felelősségről és a 85/374/EGK tanácsi irányelv hatályon kívül helyezéséről (a továbbiakban: termékfelelősségi irányelv)

²³ Az Európai Parlament és a Tanács 2005/29/EK irányelve a belső piacon az üzleti vállalkozások fogyasztókkal szemben folytatott tisztességtelen kereskedelmi gyakorlatairól, valamint a 84/450/EGK tanácsi irányelv, a 97/7/EK, a 98/27/EK és a 2002/65/EK európai parlamenti és tanácsi irányelvek, valamint a 2006/2004/EK európai parlamenti és tanácsi rendelet módosításáról (a továbbiakban: UCP-irányelv)

szabályozás nem a koherencia, hanem a széttöredezettség irányában hat. A fogyasztóvédelmi jogba integrált nagyszámú adatvédelmi rendelkezés és a koherenciaproblémák megoldásának szükségessége akár sajátos szabályozási terület kialakulásához is vezethet.

Feltételezésem szerint az EU fogyasztóvédelmi eszközrendszere hozzájárul a fogyasztók személyes adatokkal kapcsolatos aszimmetrikus helyzetének mérsékléséhez, de nem képes azt teljes mértékben felszámolni; ami arra is utalhat, hogy sajátos szabályozási terület, a fogyasztóvédelmi adatjog van kialakulóban.

Az egyes fejezetek felépítését tekintve az egységességre törekedtem. A négy kérdéskörhöz kapcsolódó, az adott fejezetre vetített kérdéseket, problémákat a fejezetek (nem alszámozott) bevezető részében konkrétan, részletesen fogalmazom meg, majd a kifejtő részben elemzést és értékelést végzek. A személyes adatok kezeléséhez kötődő fejezetekben a kifejtéshez szorosan hozzátartozik az is, hogy kitekintsek a versenyjog és a fogyasztóvédelem területére, ezáltal előrevetítsek olyan megközelítési lehetőségeket, amelyek rámutatnak a metszéspontokra. Az egyes fejezeteket összegzéssel és következtetésekkel zárom. Feltétlenül szükségesnek ítélttem meg, hogy táblázatokkal és ábrákkal támasszam alá elemzésemet, ezek a dolgozat főszövegében, valamint a mellékletekben kaptak helyet, de utóbbi esetben is utalok a szerepükre.

A dolgozat fő fejezeteit követő zárórészben, az Összegző gondolatok, következtetések című fejezetben a felvázolt kérdések és hipotézisek mentén haladok. Ebben a részben már nem használok hivatkozásokat, azok a kifejtő részekben szerepelnek.

3. A kutatás módszerei

Alapvetően a jogszabáyelemző és -összehasonlító módszert alkalmazom, értve ezt a jogszabályjavaslatokra is. A személyes adatok kezelése tekintetében az érintettek és a felhasználók védelmén örökődő uniós jogszabályokat – különösen a GDPR-t és az elektronikus hírközlési adatvédelmi irányelvet – mélységében elemzem, igyekszem a háttérben munkáló miértekre összpontosítani. A célom az, hogy rámutassak, e jogszabályok képesek-e teljes körű védelmet biztosítani az érintetteknek és a felhasználóknak, ezért ezek minél részletesebb vizsgálatára törekszem, ideértve az összefüggések feltárását is. Ehhez a jogforrások normaszövegét tartom alapvető fontosságúnak, továbbá a kapcsolódó uniós dokumentumokat, amelyek az értelmezéshez hozzájárulhatnak, úgymint a 29. cikk szerinti adatvédelmi

munkacsoport, ill. az EDPB iránymutatásait,²⁴ valamint a vonatkozó nagyszámú szakirodalom eredményeit.

Mind a GDPR, mind az elektronikus hírközlési adatvédelmi irányelv lehetőséget ad arra, hogy a jogszabály-összehasonlító módszerrel előre- és hátra is tekintsek. Ezzel a jogalkotási folyamat ívét, a jogalkotói szándék formálódását is igyekszem láttatni, összefüggésben azokkal a tényezőkkel, amelyek a digitális gazdaság fejlődéséből következtek és következnek. Mind a jogszabályelemző, mind az összehasonlító módszert az említett két uniós jogforráson kívül a versenyjogi (DMA, Data Act) és a fogyasztóvédelmi eszközrendszer (pl. DSA, UCP-irányelv) elemeire vonatkozóan is alkalmazom. Ez lehetőséget biztosít a jogalkotási aktusok összefüggéseinek átlátására, és annak megállapítására, hogy az uniós lépések mennyire összehangoltak és koherensek.

A kutatáshoz szükségesnek láttam, hogy az előzőektől kisebb mértékben, de támaszkodjam a történeti módszerre is. Az adatvédelem és az adatvédelmi jog fejlődését röviden tekintem át, ezáltal emelve ki azokat a mozgatórugókat és a szabályozás folyamatából eredő sajátosságokat, amelyek elvezettek az EU mai adatvédelmi szabályozásához.

A jogszabályok gyakorlati szempontú megközelítését fontosnak tekintem, ezért nagyszámú kapcsolódó jogesetet vizsgálok, mind a Európai Unió Bírósága (a továbbiakban: EUB) esetjogából, mind a hazai bírósági és hatósági eljárásokból. Törekszem arra, hogy a klasszikus példákon kívül az újabbak is fókuszba kerüljenek, és következtetést vonjak le általuk. A jogalkalmazást konkrét példákon keresztül bemutatva elérhető az a cél, hogy megállapításokat tegyek az adatvédelem, a versenyjog és a fogyasztóvédelem területén az ellenőrzési, végrehajtási kérdésekre vonatkozóan, valamint az EU jogalkotási folyamatait motiváló tényezőkre.

²⁴ Article 29 Data Protection Working Party: '29. cikk alapján létrehozott adatvédelmi munkacsoport' (a továbbiakban a lábjegyzetekben dokumentum azonosítóelemeként: WP. Szerepét 2018-tól a European Data Protection Board (a továbbiakban: Európai Adatvédelmi Testület/EDPB) vette át.

I. FEJEZET: FOGALMI MEGKÖZELÍTÉSEK ÉS AZ ADATVÉDELEM TÖRTÉNETE

A dolgozat témája szempontjából elengedhetetlenül fontos annak tisztázása, hogy kit tekintünk fogyasztónak. Az Európai Unió működéséről szóló szerződésben rögzített fogyasztói érdekek védelme céljából az EU fogyasztóvédelmi intézkedéseket fogad el,²⁵ amelyek több jogszabályban kaptak és kapnak helyet. E másodlagos jogforrások az adott jogviszonnyal összefüggésben értelmezik a fogyasztó fogalmát is, ami a jogalkalmazók szempontjából rendkívül fontos, hiszen a lefektetett definíció teremt alapot a normaszöveg egységes értelmezésére, legelsősorban a meghatározás fogja eldönteni, hogy a szabályozás vonatkozik-e a vizsgált jogügylet alanyára. A fogyasztó fogalmának körüljárása során arra keresem a választ, hogy az biztosít-e egységes, stabil normát vagy legalább megközelítést a széttagolt fogyasztóvédelmi intézkedések koherenciájának előmozdítása érdekében. További kérdésként merül fel az, hogy a fogyasztói magatartás differenciált megközelítése tekintetében milyen viszonyítási alapot alkalmaz az EU, valamint hogy milyen fogyasztói csoportokat részesít erősebb védelemben. Lényeges kérdésként fogalmazódik meg az is, hogy a digitális piacon, az online térben a fogyasztófogalom magában foglal-e minden olyan elemet, amely lehetőséget biztosít a fogyasztók tényleges védelmére.

1. A fogyasztó fogalma

A vonatkozó jogszabályok hasonló elv mentén definiálják a fogyasztó fogalmát, először a jogalanyiség szempontjából minősítik, majd a szakmai tudással rendelkező, erősebb félhez viszonyítva, annak ellentétéként, a különbség mentén töltik meg tartalommal. A különbség, ami alapján a szembeállítás történik, a célban ragadható meg.

Az alábbi, 1. táblázat több jogforrás alapján mutatja a fogyasztó fogalmának definícióit, figyelemmel azokra a feltételekre, amelyeknek együttesen kell érvényesülniük e fogalom meghatározásakor. A lista nem öleli fel a fogyasztóvédelem teljes joganyagát, a táblázatban szereplő jogszabályok többsége olyan fogyasztóvédelmi és versenyjogi uniós jogforrás, amely később szerepet kap dolgozatomban; kisebb része a fogyasztói helyzet sokrétűségéből következően a jogalanyok árnyaltabb megközelíthetőségét teszi lehetővé, ezáltal a fogyasztófogalom fejlődési irányára is rámutathat. Mivel e jogszabályok között több irányelv

²⁵ Az Európai Unióról szóló szerződés és az Európai Unió működéséről szóló szerződés egységes szerkezetbe foglalt változata (a továbbiakban: EUMSZ) 169. cikk

is van, és azok a tagállami, így a magyar joganyagba is implementáció által illeszkedtek be, ezért a táblázat a vonatkozó magyar jogszabályok definícióit is tartalmazza.

1. táblázat: A fogyasztó fogalma az uniós és a magyar jogszabályokban

Jogszabály	Jogalany	Cél szerint
DSA 3. cikk c) pont	természetes személy	kereskedelmi, üzleti, kézműipari vagy szakmai tevékenységén kívül eső célokból/célok érdekében jár el
Data Act 2. cikk 23. pont		
UCT-irányelv ²⁶ 2. cikk b) pont		aki az ezen irányelv(ek) hatálya alá tartozó esetekben saját szakmája, foglalkozása, kereskedelmi, ipari, kézműipari, üzleti tevékenysége körén kívül jár el
CR-irányelv ²⁷ 2. cikk 1. pont és (17) preambulumbekkezdés		
DCS-irányelv 2. cikk 6. pont		
UCP-irányelv 2. cikk a) pont		
Geo-blocking rendelet ²⁸ 2. cikk 12. pont 2. cikk 13. pont		aki olyan célból jár el, amely kívül esik kereskedelmi, ipari, kézműipari vagy szakmai tevékenysége körén
	=vevő: az a vállalkozás is, amely valamely tagállamban letelepedési hellyel rendelkezik	és az Unión belül kizárólag végfelhasználás céljából vásárol árut vagy vesz igénybe szolgáltatást, vagy ilyen szándékkal jár el
Utazási csomagokról szóló irányelv ²⁹ 3. cikk 6. pont	=utazó: személy	akinek szándékában áll egy, ezen irányelv hatálya alá tartozó szerződés megkötése, vagy ilyen szerződés alapján utazásra jogosul

²⁶ A Tanács 93/13/EGK irányelve (1993. április 5.) a fogyasztókkal kötött szerződésekben alkalmazott tisztességtelen feltételekről (a továbbiakban: UCT-irányelv)

²⁷ Az Európai Parlament és a Tanács 2011. október 25-i 2011/83/EU irányelve a fogyasztók jogairól, a 93/13/EGK tanácsi irányelv és az 1999/44/EK európai parlamenti és tanácsi irányelv módosításáról, valamint a 85/577/EGK tanácsi irányelv és a 97/7/EK európai parlamenti és tanácsi irányelv hatályon kívül helyezéséről (a továbbiakban: CR-irányelv)

²⁸ Az Európai Parlament és a Tanács (EU) 2018/302 rendelete (2018. február 28.) a belső piacon belül a vevő állampolgársága, lakóhelye vagy letelepedési helye alapján történő indokolatlan területi alapú tartalomkorlátozással és a megkülönböztetés egyéb formáival szembeni fellépésről, valamint a 2006/2004/EK és az (EU) 2017/2394 rendelet, továbbá a 2009/22/EK irányelv módosításáról (a továbbiakban: Geo-blocking rendelet)

²⁹ Az Európai Parlament és a Tanács (EU) 2015/2302 irányelve (2015. november 25.) az utazási csomagokról és az utazási szolgáltatássegítesekről, valamint a 2006/2004/EK rendelet és a 2011/83/EU európai parlamenti és tanácsi irányelv módosításáról, továbbá a 90/314/EGK tanácsi irányelv hatályon kívül helyezéséről (a továbbiakban: utazási csomagokról szóló irányelv)

45/2014. (II. 26.) kormányrendelet ³⁰ 4. § 2. pont	Ptk.-ra utalással: (természetes személy)	(a szakmája, önálló foglalkozása vagy az üzleti tevékenysége körén kívül jár el)
Ptk. ³¹ 8:1. § (1) bekezdés 3. pont	természetes személy	a szakmája, önálló foglalkozása vagy az üzleti tevékenysége körén kívül jár el
Fttv. ³² 2. § a) pont		önálló foglalkozásán és gazdasági tevékenységén kívül eső célok érdekében jár el (e törvény alkalmazásában)
Fgy. tv. ³³ 2. § 10. pont		- aki az önálló foglalkozásán és gazdasági tevékenységén kívül eső célok érdekében jár el, - aki árut vesz, rendel, kap, használ, igénybe vesz vagy az áruval kapcsolatos kereskedelmi kommunikáció, ajánlat címzettje
Fgy. tv. 2. § 10. pont a békéltető testületre vonatkozó szabályok alkalmazásában a fentiekén túlmenően	civil szervezet, egyházi jogi személy, társasház, lakásszövetkezet	- amely az önálló foglalkozásán és gazdasági tevékenységén kívül eső célok érdekében jár el - amely árut vesz, rendel, kap, használ, igénybe vesz vagy az áruval kapcsolatos kereskedelmi kommunikáció, ajánlat címzettje
	=vevő: az a vállalkozás is, amely valamely tagállamban letelepedési hellyel rendelkezik	és az Unión belül kizárólag végfelhasználás céljából vásárol árut vagy vesz igénybe szolgáltatást, vagy ilyen szándékkal jár el

Forrás: saját szerkesztés az első oszlopban felsorolt jogszabályok alapján

A táblázat alapján leszűrhető következtetések a következők: egyrészt a fogyasztót nem egységesen definiálják a fogyasztóvédelmi intézkedéseket tartalmazó európai és magyar jogszabályok, másrészt két közös elem mégis kiemelhető belőlük: 1.) fogyasztónak általában a természetes személyt tekintik, 2.) aki önálló foglalkozásán és gazdasági tevékenységén kívül eső célok érdekében jár el.

A természetes személy minősítés azt jelenti, hogy a nem természetes személyek, a jogi személyek nem tartoznak a fogyasztók körébe. Konzekvensen kitart e felfogás mellett az EUB

³⁰ 45/2014. (II. 26.) Korm. rendelet a fogyasztó és a vállalkozás közötti szerződések részletes szabályairól (a továbbiakban: 45/2014. (II. 26.) kormányrendelet)

³¹ 2013. évi V. törvény a Polgári Törvénykönyvről (a továbbiakban: Ptk.)

³² 2008. évi XLVII. törvény a fogyasztókkal szembeni tisztességtelen kereskedelmi gyakorlat tilalmáról (a továbbiakban: Fttv.)

³³ 1997. évi CLV. törvény a fogyasztóvédelemről (a továbbiakban: Fgy. tv.)

is,³⁴ még akkor is, ha a jogi személyek adott jogügyletben a természetes személyekhez hasonlóan hátrányos pozícióban vannak. Erre a kettősségre mutat rá annak a milánói condominiának, társasháznak az ügye, amelynek közös képviselője hőenergia-ellátási szerződést kötött az Eurothermóval, ami alapján késedelmes fizetés esetén az adóst 9,25%-os késedelmi kamat terheli. A kapott fizetési meghagyással szemben a közös képviselő – fogyasztóként értelmezve a társasházat – a szerződésben kikötött kamatfizetésre mint tisztességtelen feltételre hivatkozott.³⁵ Az előzetes döntéshozatali kérelemre született EUB-ítélet megállapította, hogy a társasház nem tartozik a fogyasztó fogalmába, mert a vonatkozó UCT-irányelv alapján³⁶ nem természetes személy.³⁷ Mindemellett ennek az irányelvnek a nemzeti jogba való átültetésére minimumharmonizációs kötelezettség vonatkozott, meghagyva a tagállamok számára azt a lehetőséget, hogy nemzeti jogszabályaikban az irányelvben előírtaknál szigorúbb rendelkezésekkel biztosítsanak magasabb szintű védelmet a fogyasztók számára. Az olasz jog szerint a társasház olyan jogalany, amely nem természetes személy, és nem is jogi személy, tehát az olasz jogszabály az e jogalany által valamely eladóval vagy szolgáltatóval kötött szerződésre akkor is alkalmazandó, ha az ilyen jogalany nem tartozik az említett irányelv hatálya alá, így a vonatkozó EUB-ítélet 2020-ban azt is megállapította, hogy az irányelvvel nem ellentétes az olasz ítélkezési gyakorlat.³⁸

Bár a felsorolt jogszabályok fogyasztónak általában a természetes személyt tekintik, ettől eltérést mutat a Geo-blocking rendelet, amely a fogyasztói pozícióban lévő jogi személyeket is védelemben részesíti. E rendelet célja az, hogy fellépjen a vevő állampolgársága, lakóhelye vagy letelepedési helye alapján történő indokolatlan területi alapú tartalomkorlátozással és a megkülönböztetés egyéb formáival szemben. Egyszerű példája lehet ennek, ha egy Németországban letelepedett kereskedő korlátozza a weboldalához hozzáférést a magyarországi vevők számára, vagy ugyanennek a vevőnek csak utánvétes fizetést kínál fel, míg a többi tagállamban tartózkodó vevők bankkártyával is fizethetnek.³⁹ A határokon átnyúló ügyletek – igazodva az egyenlő bánásmód és a megkülönböztetésmentesség céljához – azt is megkövetelik, hogy a tagállamok nemzeti hatóságai együttműködésének biztosítása érdekében

³⁴ HAJNAL Zsolt: *A fogyasztói jogok egységes európai szabályozásának lehetséges irányai*. Doktori értekezés, Debrecen, 2013. 61.

³⁵ ECLI:EU:C:2020:263. A Bíróság ítélete (első tanács) a C-329/19. sz. ügyben (Condominio di Milano, via Meda és az Eurothermo SpA ügy), 2020. április 2. 14–16. pont (a továbbiakban a lábjegyzetekben: EUB-ítélet C-329/19. sz. ügy)

³⁶ UCT-irányelv 2. cikk b) pont

³⁷ Az EUB által vizsgált, sokat idézett, mára klasszikusnak tekinthető jogesetek: EU:C:2001:625. C-541/99. sz. ügy (Cape Snc v. Idealservice Srl) és C-542/99. sz. ügy (Idealservice MN RE Sas v. OMAI Srl)

³⁸ EUB-ítélet C-329/19. sz. ügy 29. és 38. pont

³⁹ Geo-blocking rendelet (1) és (22) preambulumbekzdés

a vevőt is fogyasztónak tekinték.⁴⁰ Ezért a Geo-blocking rendelet a vevők közül fogyasztónak tekinti a következő két csoportba tartozókat: aki valamely tagállam állampolgára, vagy valamely tagállamban lakóhellyel rendelkezik; valamint – mivel gyakran hasonló helyzetben vannak, mint a fogyasztók – azt a vállalkozást is, amely valamely tagállamban letelepedési hellyel rendelkezik, de csak abban az esetben, ha végfelhasználás a vásárlás célja,⁴¹ tehát a viszonteladókra, továbbfeldolgozó vállalkozásokra nem vonatkozik. Ezzel a Geo-blocking rendelet – tekintve, hogy a vállalkozások jellemzően jogi személyek – a természetes személyek mellett a jogi személyek egy részét is beilleszti a fogyasztók körébe.

A Geo-blocking rendelet tagállami átültetése miatt az Fgy. tv.– a békéltető testületre vonatkozó szabályok alkalmazásában – szintén fogyasztónak minősíti a valamely tagállamban letelepedési hellyel rendelkező végfelhasználó vállalkozásokat,⁴² akkor is, ha azok jogi személyek. Az Fgy. tv. ugyanebben a vonatkozásban fogyasztónak tekinti a civil szervezetet, az egyházi jogi személyt, a társasházat és a lakásszövetkezetet,⁴³ amelyek egy része szintén a jogi személyek közé tartozik. Ugyanígy az utazási csomagokról szóló irányelv definíciója – amely a védelemben részesülő személyeket nem fogyasztónak nevezi, hanem az utazó fogalmat használja⁴⁴ – jogalanyként a személyt nevezi meg,⁴⁵ aki/ami akár jogi személy is lehet.

Az, hogy a Geo-blocking rendelet és az utazási csomagokról szóló irányelv a természetes személyek mellett a jogi személyeket is védelemben részesíti, arra utal, hogy a jogalanyok körét indokolt esetben a jogalkotó kitágítja. Mindkét jogszabály esetében a kiszolgáltatott piaci helyzet a motiváló tényező, vagyis a gyengébb felet nem a biológiai adottságok, nem a természetes személy lét alapján értékeli, hanem az alapján, hogy – ha például egy kis vállalkozás informatikai eszközt vásárol a saját irodájába, vagy ha üzleti utat vásárol – ugyanolyan információs aszimmetriával és kedvezőtlen alkupozícióval szembesül, mint a természetes személy. A Geo-blocking rendelet esetében két indokot lehet azonosítani a nem

⁴⁰ Geo-blocking rendelet (38) preambulumbekkezdés

⁴¹ Geo-blocking rendelet 2. cikk 13. pont

⁴² Fgy. tv. 2. § 10. pont

⁴³ Fgy. tv. 2. § 10. pont

⁴⁴ Az utazási csomagokról szóló irányelvet a magyar jogba több jogszabály által implementálták, idetartozik a 472/2017. (XII. 28.) Korm. rendelet az utazási szolgáltatásokra vonatkozó szerződésekről, különösen az utazási csomagra és az utazási szolgáltatás együttesre vonatkozó szerződésekről. Ennek „utazó” fogalmát a kereskedelemről szóló 2005. évi CLXIV. törvény 2. § 37. pontja határozza meg („minden olyan személy, akinek szándékában áll utazási szolgáltatásra vagy azok összeállítására vonatkozó szerződés megkötése, vagy ilyen szerződés alapján utazásra jogosult”), de a Ptk. – a kétféle fogyasztófogalom használatának elkerülése érdekében – az utazási szerződést nem fogyasztói szerződésnek szabályozza, hanem utazási szerződésnek (6:254. §), amelyben megrendelő bárki lehet. Az utazási csomagokról szóló irányelv által biztosított védelem ezért változatlanul megilleti a Ptk. szerinti bármely megrendelőt: „A díjengedmény, illetve a kártérítési igény elévülése szempontjából a fogyasztónak nem minősülő megrendelőt is fogyasztónak kell tekinteni.” (Ptk. 6:254. § (2) bekezdés).

⁴⁵ Utazási csomagokról szóló irányelv 3. cikk 6. pont

természetes személyek védelme mellett: egyrészt a végfelhasználói helyzethez, az ügylet/tranzakció céljához kötődik a védelem; másrészt a piaci széttagoltság megszüntetéséhez, az egységes piac megteremtéséhez is hozzájárul.

A fogyasztófogalom meghatározásának – a jogalanyra vonatkozó besorolás mellett – másik eleme a valamely gazdasági szereplőhöz viszonyított céljai mentén ragadható meg. A gazdasági szereplő jellemzően a kereskedő, de lehet az eladó vagy a szolgáltató is, mindegyiknek közös vonása az, hogy szakmabeli, ezért több tudással, ismerettel bír, mint a fogyasztó. Ebből következik a fogyasztófogalom definíciójának másik lényeges eleme: gazdasági tevékenysége, szakmája, önálló foglalkozása vagy üzleti tevékenysége körén kívül eső célokból jár el. A vizsgált jogszabályok mindegyike ezt a meghatározást tartalmazza, az Fgy. tv. azonban hozzáteszi még: „aki árut vesz, rendel, kap, használ, igénybe vesz, vagy az áruval kapcsolatos kereskedelmi kommunikáció, ajánlat címzettje.” Fogyasztónak minősül tehát az is, aki például ajándékba kapta az árut, vagy aki pusztán árajánlatot kért, vagyis „a jogügyleti szituáció dönt a fogyasztói minőség megítéléséről,”⁴⁶ ami által a jogalkotó jelentősen ki is tágította a fogalom jelentését.

A CR-irányelv alapján a kettős célú szerződések esetében – amelyeknél a szerződést részben a személy szakmájába tartozó, részben azon kívül eső célból kötik – adott személy csak abban az esetben tekinthető fogyasztónak, ha „a kereskedési cél annyira korlátozott, hogy a teljesítés egésze szempontjából nem elsődleges.”⁴⁷ Ezt támasztja alá a következő EUB-ítélet: a Comtrans fuvarozócég vezetője, LB hitelt vett fel a FAER pénzügyi társaságtól, és LB édesanyja lakására jelzálogot alapítottak. A fizetéseképtelenségi eljárás során a cégvezető testvére, MB vett fel újabb hitelt a korábbi hitelek visszafizetésére, majd miután ő sem tudott törleszteni, a kényszervégrehajtás ellen kifogással élt. Az EUB szerint a jogvita eldöntése a nemzeti bíróság feladata lesz, de a benyújtott iratok alapján MB fogyasztónak tekinthető, mert természetes személy, nincs nyilvánvaló kapcsolata a céggel, és a hitelfelvétel során nem szakmai tevékenységével összefüggésben járt el, hanem rokoni segítséget kívánt nyújtani édesanyjának és testvérének.⁴⁸

Előrevetítve dolgozatom későbbi fejezeteit, a digitális piacokon a gyengébb felet gyakran részesíti a fogyasztóhoz hasonló védelemben a jogalkotó, anélkül, hogy az fogyasztó

⁴⁶ HAJNAL Zsolt: *A fogyasztóvédelem alanya: a fogyasztó*. In: SZIKORA Veronika (szerk.): *Magyar fogyasztóvédelmi magánjog – európai kitekintéssel*. Debrecen, Fogyasztóvédők Magyarországi Egyesülete, 2010. 40.

⁴⁷ CR-irányelv 2. cikk 1. pont és (17) preambulumbekzdés

⁴⁸ ECLI:EU:C:2017:321. A Bíróság ítélete a C-535/16. sz. ügyben (Michael Tibor Bachman kontra FAER IFN SA), 2017. április 27.

lenne. A kapuőrök megregulázását és a tisztességes piaci versenyfeltételeket célzó DMA alapján az üzleti felhasználók a fogyasztókhoz hasonló védelemben részesülnek a kapuőrökkel szemben. Ezáltal a DMA nemcsak a versenyfeltételeket javítja, és nemcsak a kisebb üzleti felhasználók piacralépési lehetőségeit segíti elő, de a klasszikus értelemben vett fogyasztókat is támogatja, hiszen nagyobb kínálatból és várhatóan kedvezőbb áron juthatnak adott termékhez vagy szolgáltatáshoz. Horváth M. András következtetése szerint: lehetséges, hogy a UPC-irányelv 2026 szeptemberétől alkalmazandó, zöld állításokkal kapcsolatos feketelistája⁴⁹ egyre fontosabbá válik majd a vállalkozási kapcsolatokban is,⁵⁰ ugyanis a hazai versenytörvény⁵¹ értelmében a megtévesztés tilalma kiterjed az üzleti partnerekre. Ez a jogi keretrendszer biztosítja, hogy a Gazdasági Versenyhivatal⁵² a vállalkozások közötti kapcsolatokba is beavatkozhasson, ha egy zöld állítás megtévesztő. Az alapelv az, hogy a piaci integritás védelme és a zöld átállás átláthatósága közérdek, amely elsőbbséget élvez az érintett fél konkrét jogi státuszával szemben.

Amellett, hogy digitális környezetben a gyengébb felet még akkor is gyakran részesíti védelemben a jogalkotó, ha az jogi személy; azt is érdemes számbavenni, hogy a fogyasztófogalom halványulóban van. Az EU gyakran az általános kategóriákat helyezi előtérbe, mint az igénybevevők, felhasználók, polgárok (DSA), a végfelhasználók (DMA), amivel elhomályosítja a fogyasztófogalomnak azt a dimenzióját, hogy a gazdasági féllel szemben szorul védelemre.⁵³ A fogyasztóvédelmi vívmányok megtartásához szükség van a fogalom központi szerepének megőrzésére, mindenekelőtt azért, hogy digitális környezetben is erre legyen építhető a két fél közötti aszimmetria mérséklése, s hogy ezáltal horizontális (ágazatfüggetlen) védelmi keretet biztosítson a gyengébb fél számára.⁵⁴

⁴⁹ Az Európai Parlament és a Tanács (EU) 2024/825 irányelve (2024. február 28.) a 2005/29/EK és a 2011/83/EU irányelv módosításáról, a fogyasztók zöld átállásban való szerepvállalásának a tisztességtelen gyakorlatokkal szembeni hatékonyabb védelem és a hatékonyabb tájékoztatás révén történő növelése tekintetében

⁵⁰ HORVÁTH M. András: *Sustainability and Competition Law in Hungary*. In: KÉLLEZI, Pranvera – KOBEL, Pierre – KILPATRICK, Bruce: *Sustainability Objectives in Competition and Intellectual Property Law*. 8. 2024. 152–154. <https://doi.org/10.1007/978-3-031-44869-0> (letöltés: 2025. 12. 30.)

⁵¹ 1996. évi LVII. törvény a tisztességtelen piaci magatartás és a versenykorlátozás tilalmáról (a továbbiakban: Tpv.) 8. §

⁵² Gazdasági Versenyhivatal (a továbbiakban: GVH)

⁵³ M. NAMYSŁOWSKA: *The Silent Death of EU Consumer Law and Its Resilient Revival: Reinventing Consumer Protection Against Unfair Digital Commercial Practices*. *Journal of Consumer Policy* 2025/48. 320. <https://doi.org/10.1007/s10603-025-09590-5> (letöltés: 2025. 12. 22.)

⁵⁴ NAMYSŁOWSKA (2025) i. m. 329–330.

1.1. Az átlagfogyasztó és a kiszolgáltató fogyasztó

A UCP-irányelv mind az átlagfogyasztóra, mind a kiszolgáltató fogyasztóra vonatkozóan tartalmaz információkat. Bár a UCP-irányelv a kereskedelmi kommunikációra, marketingre, reklámozásra vonatkozó szabályokat tartalmaz, de mindkét említett fogalmat kifejezetten és implicit módon használták a fogyasztóvédelem más területein is.⁵⁵ Az átlagfogyasztó fogalmat az EUB dolgozta ki a reklámra vonatkozó ítélkezési gyakorlatában a feltételezett, tipikus fogyasztóra gyakorolt hatás vizsgálatára,⁵⁶ majd a fogalmat a UCP-irányelv egységesítette, „hogy közös kritériumokat biztosítson a nemzeti hatóságok és bíróságok számára a jogbiztonság megerősítése, valamint az eltérő értékelések lehetőségének csökkentése érdekében.”⁵⁷

Az átlagfogyasztó jelentését az uniós jogszabályok közül egyedül a UCP-irányelv határozza meg, és a fogyasztói szituációban elvárható tipikus jellemzőket, magatartásmintákat⁵⁸ tartalmazza. Eszerint az átlagfogyasztó „megfelelően tájékozott, figyelmes és körültekintő,” de az adott tagállamra, piacra vonatkozó társadalmi, kulturális és nyelvi tényezőket is figyelembe kell venni.⁵⁹ E megállapítások nem statisztikai alapúak, a konkrét esetben tanúsított átlagfogyasztói magatartást a nemzeti bíróságok és hatóságok – az EUB esetjogát figyelembe véve – saját jogkörükben határozhatják meg.⁶⁰ Lényegében a UCP-irányelv megközelítését veszi át az Fttv. is – de az átlagfogyasztó szó használata nélkül –, amikor olyan fogyasztó magatartásának alapul vételét írja elő, aki tájékozódás, figyelem és körültekintés tekintetében szélsőségektől mentesen jár el, és emellett nyelvi, kulturális és szociális vonatkozásokat is figyelembe kell venni.⁶¹

Az átlagfogyasztói magatartás értelmezését a tagállami sajátosságok (társadalmi, kulturális és nyelvi tényezők) is befolyásolhatják, ezt az EUB többször megerősítette. Erre

⁵⁵ PE 690.619. Nikolina ŠAJN: *Briefing EPRS (European Parliamentary Research Service): Vulnerable consumers*, 2021. május. 2.

⁵⁶ UCP-irányelv (18) preambulumbekkezdés. Ez egyben arra is utal, hogy a fogyasztófogalom specifikációja eredetileg három kategóriát tartalmazott: átlagfogyasztó, megcélzott átlagfogyasztó és kiszolgáltató fogyasztó. A UCP-irányelvben azonban már egyesítették a kiszolgáltató fogyasztóra és a megcélzott átlagfogyasztóra vonatkozó rendelkezéseket. PE 690.619. ŠAJN i. m. 4., valamint Natali HELBERGER et al.: *EU Consumer Protection 2.0: Structural asymmetries in digital consumer markets: A joint report from research conducted under the EUCP2.0 project*. 2021. március. 1. https://www.beuc.eu/sites/default/files/publications/beuc-x-2021-018_eu_consumer_protection_2.0.pdf (letöltés: 2023. 12. 20.)

⁵⁷ 2021/C 526/01. A Bizottság közleménye – Iránymutatás a belső piacon az üzleti vállalkozások fogyasztókkal szemben folytatott tisztességtelen kereskedelmi gyakorlatairól szóló 2005/29/EK európai parlamenti és tanácsi irányelv értelmezéséhez és alkalmazásához. 2.5. Átlagfogyasztó

⁵⁸ HAJNAL (2013) i. m. 66.

⁵⁹ UCP-irányelv (18) preambulumbekkezdés

⁶⁰ UCP-irányelv (18) preambulumbekkezdés

⁶¹ Fttv. 4. § (1) bekezdés

vonatkozóan az Estée Lauder kontra Lancaster ügyben az EUB rögzítette, hogy a fogyasztót megtévesztheti, félrevezetheti az adott kozmetikai krém nevében szereplő lifting ('bőrfeszítő') szó használata, mert az olyan jellemzőre utal, amilyen jellemzővel a termék nem rendelkezik. Noha az átlagos fogyasztó észszerűen tájékozott, figyelmes és körültekintő, ezért nem számíthat arra, hogy az akár a terméken, akár a reklámban megjelenő „lifting” jelző a krém tartós hatását jelentené, ugyanakkor azonban társadalmi, kulturális vagy nyelvi tényezők indokolhatják a kozmetikai krém „lifting” minősítését, amely mást jelenthet a német fogyasztó számára, mint a többi tagállam fogyasztói számára; ennek mérlegelése és eldöntése a tagállami bíróság feladata, amihez akár szakértői vélemény vagy közvélemény-kutatás igénybevétele is szükséges lehet.⁶² Adott ügy rámutat arra is, hogy a fogyasztónak joga van a tájékoztatáshoz, és az információkat értékelni is tudja,⁶³ ill. arra is, hogy a megtévesztő tájékoztatás a piaci versenyben is szerepet játszik. Egy másik ügyben az EUB úgy ítélte meg, hogy a németországi átlagfogyasztót nem fogja megtéveszteni a kozmetikai termék Clinique márkanéve, és nem fogja azt gyógyászati terméknek tekinteni, még akkor sem, ha a német nyelvben a kórház jelentés asszociálódik hozzá, ezért nem indokolt a márkanév használatának megtiltása.⁶⁴

A UCP-irányelv az átlagfogyasztó mellett a fogyasztók kiszolgáltatott, egyértelműen azonosítható csoportját is megkülönbözteti, mert a tisztességtelen kereskedelmi gyakorlatok e csoportot még hatványozottabban érinthetik, ezért számukra nagyobb fokú védelmet kell biztosítani. A kiszolgáltatottság oka szellemi vagy fizikai fogyatékoságuk, koruk vagy hiszékenyséjük lehet, mércéje pedig az, hogy a kereskedő által észszerűen előre látható,⁶⁵ vagyis csak akkor hárul a kereskedőre a felelősség, ha az előre láthatta a kiszolgáltatott csoportra gyakorolt tisztességtelen hatást.⁶⁶ A felsorolt okok közül a legbizonytalanabb jelentésű fogalom a hiszékenység, amelynek absztrakciós szintje olyan mértékű, hogy valamely magatartás vizsgálata során akár bírói értelmezést is igényelhet, nem szolgálva ezzel „a jogalkotói cél hatékony érvényesülését.”⁶⁷ Az olasz verseny- és fogyasztóvédelmi hatóság (Autorità Garante della Concorrenza e del Mercato, a továbbiakban: AGCM) egy olyan céget bírságolt meg, amely fogyásegítő és más gyógyhatású termékeket megtévesztő és

⁶² ECLI:EU:C:2000:8. A Bíróság (ötödik tanács) ítélete a C-220/98. sz. ügyben (Estée Lauder Cosmetics GmbH & Co. OHG v Lancaster Group GmbH), 2000. január 13.

⁶³ HAJNAL Zsolt: *A fogyasztói szerződések joga az Európai Unió jogában: közös alapok*. Debreceni Jogi Műhely 2014/1–2. 2.

⁶⁴ ECLI:EU:C:1994:34. A Bíróság (ötödik tanács) ítélete a C-315/92. sz. ügyben (Verband Sozialer Wettbewerb eV kontra Clinique Laboratoires SNC et Estée Lauder Cosmetics GmbH), 1994. február 2.

⁶⁵ UCP-irányelv (18) preambulumbekzdés, 5. cikk (3) bekezdés

⁶⁶ 2021/C 526/01. 2.6. Kiszolgáltatott fogyasztók

⁶⁷ BENCZE Máttyás: *A viselkedéstudományok eredményeinek hasznosíthatósága a hazai fogyasztóvédelmi jog területén*. In: SZIKORA Veronika – ÁRVA Zsuzsanna (szerk.): *A fogyasztók védelmének új irányai és kihívásai a XXI. században*. Debrecen, Debreceni Egyetem Állam- és Jogtudományi Kar, 2018. 180.

összehasonlító módon reklámozott és forgalmazott, s ezzel jelentősen torzította a fogyasztók gazdasági döntéseit. A hatóság figyelembe vette a reklámok hatásait a beteg és túlsúlyos csoportba tartozók átlagos tagjának magatartására vonatkozóan, akik a fizikai, ill. pszichés helyzetükből adódóan különösen sérülékenyek és ezáltal fogékonyak ezekre.⁶⁸

A kiszolgáltatott, egyértelműen azonosítható fogyasztói csoportot az Fttv. is megkülönbözteti, a UCP-irányelvvel azonos szempontok alapján; ideértve azt is, hogy a kereskedő akkor tehető felelőssé, ha általa észszerűen előre látható volt, hogy a kereskedelmi gyakorlat a sérülékeny csoport magatartására torzító hatást gyakorol.⁶⁹ A GVH versenytanácsa a Global AQA tinédzsereket érintő témákkal foglalkozó Bongo szolgáltatását vizsgálta, amelynek lényege, hogy az igénybe vevő sms-ben elküldi a kérdését és néhány adatot, majd személyre szabott választ kap Bongótól, a kismajomtól. A GVH megállapította, hogy a marketingismeretekkel rendelkező vállalkozásnak tisztában kellett lennie azzal, hogy a szolgáltatásuk és annak reklámja a sérülékeny, kiszolgáltatott gyermekeket célozta meg és ösztönözte vásárlásra, miközben félrevezetően hirdették a szolgáltatás árát. Szintén tudnia kellett a szolgáltatónak (és a közvetítőknek is) azt, hogy a célcsoport többsége okostelefont használ, így az apróbetűs információk nehezen vagy egyáltalán nem észlelhetők, ezzel szemben a telefonszám, amire az sms-t kellett küldeni, kiemelt betűmérettel szerepelt. A fogyasztóvédelmi szempontok kapcsolódó adatvédelmi kérdéseket is feltártak: adatkezelési tájékoztatás és szerződés nélkül is igénybe vehető volt a szolgáltatás, ha a gyerekek megadták a kért személyes adatokat.⁷⁰

A kiszolgáltatott fogyasztók tekintetében a tájékoztatási kötelezettségre vonatkozóan – a távollévők között kötött és az üzlethelyiségen kívül kötött szerződések tekintetében – a CR-irányelv is releváns, eszerint „a kereskedőnek figyelembe kell vennie azon fogyasztók egyedi szükségleteit, akik szellemi, testi vagy pszichés fogyatékoságuk, koruk vagy hisztériájuk miatt különösen kiszolgáltatottak,”⁷¹ amit a tájékoztatási kötelezettség harmonizációja érdekében Magyarországon a 45/2014. (II. 26.) kormányrendeletbe ültettek át. A kiszolgáltatott fogyasztó kifejezést szintén nem használja, de a UCT-irányelv is utal rá, amikor a jóhiszeműség követelménye alapján különös figyelmet vár el a szerződő felek alkupozíciójának erősségére vonatkozóan.⁷²

⁶⁸ PS6980. Autorità Garante della Concorrenza e del Mercato, 2013. november 06. 46., 53., 61. pontok

⁶⁹ Fttv. 4. § (2) bekezdés

⁷⁰ Vj-3/2020/247.

⁷¹ CR-irányelv (34) preambulumbekkezdés

⁷² UCT-irányelv preambuluma

1.2. Az átlagfogyasztó a digitális környezetben

Tovább árnyalja a képet az, hogy az átlagfogyasztóhoz rendelt jellemzők mennyire állják meg a helyüket a digitális környezetben, különösen az online platformok világában. Egyrészt számolni kell az offline világban is fennálló, ún. információs aszimmetriával, amely abból az egyensúlyhiányból fakad, hogy a gazdasági szereplő többet tud szakmailag, mint a fogyasztó, de emellett az aszimmetriát táplálja maga az online tér is. Az online platformok a részükre átadott vagy más forrásból összegyűjtött személyes adatokat különböző technikákkal állítják a saját szolgálatukba – automatizált döntéshozatal, profilozás, algoritmusok, kikövetkeztetett adatok –, ezáltal mindent tudnak a fogyasztókról, a fogyasztói csoportokról. Az átlagfogyasztó hiába észszerűen tájékozott, figyelmes és körültekintő, ettől még nem fogja megérteni az előzőekben felsorolt műveletek lényegét és azok magánéletére gyakorolt hatásait. A digitális környezetben a hagyományos információs aszimmetria keretein túl megjelenik az online térrel és a platformok használatával összefüggő, elsősorban az informatikai-technológiai szakmai ismeretek hiányából fakadó aszimmetrikus viszony, amelyet digitális aszimmetriának neveznek. A digitális aszimmetria sérülékennyé teheti az átlagfogyasztót is, ezért a fogyasztóvédelem megerősítése, az aszimmetrikus helyzet új megközelítése szükséges.

Ennek az új megközelítésnek abból a felismerésből kell fakadnia, hogy nem bizonyos csoportok vagy egyének sebezhetőségét kell kezelni, hanem a digitális környezet gyakorlataira kell helyezni a hangsúlyt, amely bárkit sebezhetővé tehet.⁷³ Egyetértve a BEUC⁷⁴ és a digitális méltányosságra vonatkozó alkalmassági vizsgálat (a továbbiakban: Fitness Check) szakértőivel: az átlagfogyasztó jelenleg használt fogalmi elemeibe szükséges lenne beépíteni az ún. digitális sérülékenységet,⁷⁵ ezáltal záródhatna az egyre nyíló olló, ami jelenleg az online platformok és a fogyasztók aszimmetrikus helyzetét mutatja. Várhatóan ezt a problémát is orvosolni fogja a digitális méltányosságról szóló törvény (Digital Fairness Act, a továbbiakban: DFA), amelynek javaslata, tervek szerint 2026 negyedik negyedévére készül el.⁷⁶ (A digitális

⁷³ HELBERGER et al. *i. m.* 25.

⁷⁴ European Consumer Organisation: Európai Fogyasztói Szervezet. A BEUC betűszó a szervezet francia nevéből (Bureau Européen des Unions de Consommateurs) származik.

⁷⁵ Centre for Strategy and Evaluation Services: Study to support the Fitness Check of EU consumer law on digital fairness and the report on the application of the Modernisation Directive (EU) 2019/2161. Final Report - Part 1. Közzétéve: 2024. október 04. 19., 21., 345. https://commission.europa.eu/publications/study-support-fitness-check-eu-consumer-law-digital-fairness-and-report-application-modernisation_en?prefLang=hu&etrans=hu (letöltés: 2024. 12. 01.); amely hivatkozik a BEUC által megrendelt kutatási jelentésre: HELBERGER et al. *i. m.* 5–27.

⁷⁶ James TAMIM: *What is the EU Digital Fairness Act (DFA)?* 2025. 12. 09. <https://digitalfairnessact.com/what-is-the-digital-fairness-act> (letöltés: 2025. 12. 30.)

sérülékenység kezelési lehetőségeire a fogyasztóvédelem eszközrendszerével és a sötét megoldásokkal összefüggésben térek majd ki, a VI. fejezet 3. pontjában.)

1.3. Összegzés és következtetés

Az uniós és hazai jogszabályok nem egységesen definiálják a fogyasztó fogalmát, olyannyira nem, hogy bizonyos jogforrások nem is fogyasztónak nevezik a fogyasztót. Bár a definíció nem egységes, annak logikája, megközelítése azonban igen: minden elemzett jogszabály előbb a jogalanyok körét határozza meg, majd a gazdasági szereplővel szembeállítva a célok mentén tesz megállapítást. Eszerint a jogalanyok köre a természetes személyekre szűkül, de néhány esetben (Geo-blocking rendelet, utazási csomagokról szóló irányelv, Fgy. tv.) a jogügyletek tartalma, valamint a szabályozás célja miatt jogi személyek is minősülhetnek fogyasztónak. E tekintetben a vonatkozó jogesetek arra is rámutatnak, hogy a tagállamok figyelembe veszik a jogi személyeknek a természetes személyekéhez hasonlóan hátrányos pozícióját, ahol az implementáció erre lehetőséget ad. A fogyasztófogalom másik feltételét tekintve egységesebb a meghatározás: a gazdasági tevékenységük, szakmájuk, önálló foglalkozásuk vagy üzleti tevékenységük körén kívül eső célokból járnak el.

A fogyasztók körén belül az átlagfogyasztóra és a kiszolgáltatót fogyasztóra vonatkozóan is találunk információt a jogszabályokban. A fogyasztói szituációban elvárható átlagos, tipikus magatartásminták és jellemzők tekintetében – az EUB esetjoga alapján – a UCP-irányelv igazít el; a kiszolgáltatót fogyasztói csoportok számára a UCP-irányelv, a CR-irányelv és a UCT-irányelv is erősebb védelmet állapít meg. Az átlagfogyasztó adott esetben tanúsított magatartásának mérlegelése a nemzeti bíróságok és hatóságok feladata, amiben – a jogesetekből leszűrhetően – kulcsszerepet játszik annak megítélése, hogy a kereskedő előre láthatta-e, hogy kereskedelmi gyakorlata befolyásolja a kiszolgáltatót fogyasztókat.

Fölmerül a kérdés, hogy a fogyasztó fogalmának jelentéstartalma milyen fejlődési irányt vehet a továbbiakban. A Geo-blocking rendelet és az utazási csomagokról szóló irányelv definíciói alapján azt látjuk, hogy a klasszikus értelemben vett fogyasztót megillető védelem normáit a jogalkotó kiterjeszti a hasonlóan védelemre szoruló jogi személyekre is, amelyek jellemzően mikro-, kis- és középvállalkozások (a továbbiakban: kkv-k). Ezen túlmenően az is megfigyelhető, hogy a digitális piacokon – versenyjogi összefüggés alapján – a gyengébb felet gyakran részesíti olyan védelemben a jogalkotó (DMA), ami a fogyasztók védelméhez hasonló.

Véleményem szerint e példák és tendenciák ellenére sem várható a fogyasztófogalom teljes átalakítása, de bizonyos szektorokban a kedvezőtlen alkupozíció kiegyenlítése, a piacra lépési korlátok lebontása, az egységes piac megteremtése és az egészséges verseny elősegítése

érdekében a fogyasztó pozíciót helyezi előtérbe az EU, és kvázi fogyasztóként „helyzetbe hozza” a védtelenebb nem természetes személyeket is. A fogyasztófogalom történeti fejlődése tekintetében fontos az is, hogy az online térben a fogyasztók és a platformok technológiai, szakmai tudása között olyan szintű az aszimmetria, hogy szinte minden átlagfogyasztót fenyeget a digitális sérülékenység, ezért – egyetértve a Fitness Check javaslatával – mindenképpen szükséges a digitális sérülékenységgel számolni, és azt jogszabályi szinten kezelni.

2. Az adatvédelmi szabályozás kialakulása és fejlődése

1890 – tanulmány a magánszférához való jogról

Az Egyesült Államokban két ügyvéd, Samuel D. Warren és Louis Brandeis A magánszférához való jog címen publikáltak egy tanulmányt, melyben arra tettek kísérletet, hogy a jogrendszeren belül helyezték el a magánszférához való jogot. Háttérként gazdasági-társadalmi folyamatokat neveztek meg: a találmányok, leginkább a fényképezés új technikája és a nyilvánosságot célzó újságírás egymásra találása oda vezetett, hogy „a sajtó behatolt a magánélet, az otthonok szent és sérthetetlen területére,” az ipari méretekben üzött pletyka üzletté vált, és átlépte „az egyedül hagyatáshoz való jogot,” „a magántulajdon és a tisztesség nyilvánvaló határait.”⁷⁷ A szerzők arra a következtetésre jutottak, hogy nem a szerződésből eredeztethető jogok, és nem a magántulajdon elve kínálja a megoldást, hanem a magánszférához való jog, ami nemcsak a fotók, hanem bármely magánügy nyilvánosságra hozatalát is megakadályozhatja.⁷⁸ Ezt csupán az érintett személy teheti meg, vagy a közlés az ő hozzájárulásával történhet⁷⁹ – szinte a GDPR-t előlegező gondolatok. Értekezésüket azzal zárták, hogy a common law, az esetjog, a bírói jogfejlesztés⁸⁰ az a fegyver, „ami az évszázadok lassú tüzeiben kovácsolódott ki,” és mindig is elismerte az ember jogát ahhoz, hogy „otthona bevehetetlen vár legyen.”⁸¹ Warren és Brandeis tanulmánya szűken értelmezte a magánszférához való jogot, de először ismerték fel és fejtették ki, „hogy a magánszférához való jog elismerése és ennek biztosítása érdekében jogi védelemre van szükség.”⁸²

⁷⁷ Samuel D. WARREN – Louis D. BRANDEIS: *A magánszférához való jog*. Információs Társadalom 2005/2. 8–9.

⁷⁸ WARREN–BRANDEIS i. m. 24–25.

⁷⁹ WARREN–BRANDEIS i. m. 29.

⁸⁰ Az angolszász jogrendszer egyik szerkezeti egysége. SIMON Éva: *Egy XIX. századi tanulmány margójára*. Információs Társadalom 2005/2. 32. 6. lj.

⁸¹ WARREN–BRANDEIS i. m. 31.

⁸² SIMON i. m. 42.

1948–1950 – a magánélet védelme a nemzetközi dokumentumokban

A Warren–Brandeis-tanulmány megjelenésétől több mint fél évszázadnak kellett eltelnie ahhoz, ideértve a világháborúk keserű tapasztalatát is, hogy nemzetközi dokumentumokban deklarálják a minden embert megillető alapjogokat. Az ENSZ Emberi Jogok Egyetemes Nyilatkozatának (a továbbiakban: EJENY) 12. cikke a magán- és a családi élet tiszteletben tartásának követelményét fogalmazta meg 1948-ban: „Senkinek magánéletébe, családi ügyeibe, lakóhelye megválasztásába vagy levelezésébe nem szabad önkényesen beavatkozni, sem pedig becsületében vagy jó hírnevében megsérteni. Minden személynek joga van az ilyen beavatkozásokkal vagy sértésekkel szemben a törvény védelméhez.”⁸³ Két évvel később, 1950-ben az Európa Tanács elfogadta az Emberi Jogok Európai Egyezményét (a továbbiakban: EJEE),⁸⁴ 8. cikke alapján: „1. Mindenkinnek joga van arra, hogy magán- és családi életét, lakását és levelezését tiszteletben tartsák. 2. E jog gyakorlásába hatóság csak a törvényben meghatározott, olyan esetekben avatkozhat be, amikor az egy demokratikus társadalomban a nemzetbiztonság, a közbiztonság vagy az ország gazdasági jóléte érdekében, zavargás vagy bűncselekmény megelőzése, a közegészség vagy az erkölcsök védelme, avagy mások jogainak és szabadságainak védelme érdekében szükséges.” Az EJEE tehát nemcsak az emberi jogok védelmének alapelveit, így a magánélethez való jogot fektette le, de az állam elleni védelmet is biztosította, végrehajtását az Emberi Jogok Európai Bírósága (strasbourgi bíróság, a továbbiakban: EJEB) felügyeli.

1970-es évek – az első adatvédelmi törvények

A korabeli technológiai fejlettség az állami szférában már lehetővé tette az állampolgárok adatairól számítógépes nyilvántartások vezetését. Németország Hessen tartományában a kormány azt tervezte, hogy létrehoz egy olyan hatalmas népesség-nyilvántartó rendszert, amely minden lakosról körülbelül hetven információt tárol, ezen adatok egyetlen azonosító számsorral, személyi számmal előhívhatók, így az állami feladatellátásban részt vevők bármikor hozzáférhetnek. Az elképzelést a „Nagy Hesseni Terv” című dokumentumban fektették le, amely akkora felháborodást keltett – az állami túlhatalomtól és/vagy a történelmi múlt tapasztalataitól tartva –, hogy a terv nem valósult meg,⁸⁵ ám „a technológia fejlődéséből

⁸³ EJENY 12. cikk

⁸⁴ Az emberi jogok és az alapvető szabadságok védelméről szóló, Rómában, 1950. november 4-én kelt egyezmény. Magyarországon kihirdette az 1993. évi XXXI. törvény

⁸⁵ SZÖKE Gergely László: *Az adatvédelem szabályozásának történeti áttekintése*. Infokommunikáció és Jog 2013/3. 109.

eredő veszélyekre adott jogi válaszlépésként”⁸⁶ 1970-ben megszületett az első adatvédelmi törvény, ezzel együtt maga az adatvédelem.⁸⁷ A technológia és a veszély Európa számos térségében érezhető volt, és több országban (Dánia, Norvégia, Franciaország, Ausztria, Német Szövetségi Köztársaság)⁸⁸ alkottak adatvédelmi jogszabályt, abban látva a védekezés lehetőségét, ami – véleményem szerint – megalapozta és előrevetítette azt a szemléletet, hogy a magánélet védelme, az adatvédelem fontos értéket fog jelenteni Európában.

1980 – irányelvek a magánélet védelméről és a személyes adatok határokon átvitelő áramlásáról

A nemzetközi dokumentumok a magánélet védelme által, abba beleértve utaltak a személyes adatok védelmére. Az 1970-es években azonban az állami szférában elterjedt számítógépes nyilvántartások miatt több tekintetben igazi áttörést jelentett a Gazdasági Együttműködési és Fejlesztési Szervezet (a továbbiakban: OECD) által kiadott ajánlás, amely már a címében utal a magánülethez tartozó, de abból már önállósult személyes adatokra is: Irányelvek a magánélet védelméről és a személyes adatok határokon átvitelő áramlásáról.⁸⁹ Jelentőségét egyfelől az adja, hogy máig élő adatkezelési elveket és érintetti jogokat fektetett le, másfelől – tekintve, hogy a kidolgozásában amerikai szakemberek is részt vettek⁹⁰ – nemzetközi szinten elősegítette a személyes adatok határokon átvitelő folyamatos és biztonságos áramlását, ezáltal a kereskedelem élénkülését, a nyitott piacgazdaság kiépítését.

Az OECD-irányelvek nemzeti alkalmazással összefüggő alapelveinek többsége megfeleltethető a GDPR adatkezelési elveinek, így a felelősségre vonhatóság az elszámoltathatóság elvével, a szándékmegjelölés a célhoz kötöttséggel. A korlátozott adatgyűjtés elve az adatkezelés jogszerűségével állítható párhuzamba, valamint az adatminőség alapelvvel együtt az adattakarékossági elvvel. Az egyéni részvétel alapelve szerint az egyénnek jogában áll „a rá vonatkozó adatokba betekintést nyerni;” „kifogásolni, és amennyiben ez a kifogásolás eredményes, az adatokat törölni, helyesbíteni, kiegészíteni vagy

⁸⁶ BÖRÖCZ István: *A személyes adatok védelmének bírósági gyakorlata Magyarországon*. Jura 2014/2. 177.

⁸⁷ BÖRÖCZ i. m. 177. hivatkozik a következő forrásra: JAKAB András (szerk.): *Az Alkotmány kommentárja* II. kötet. Bp., Századvég Kiadó, 2009. 2169.

⁸⁸ SZÖKE (2013) i. m. 109. hivatkozik a következő forrásra: HEGEDŰS Bulcsú: *Az adatvédelmi jog általános tanai*. In: TÓTH András (szerk.): *Az infokommunikációs jog* II. Patrocínium, 2013. 137.

⁸⁹ OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data (1980). Kivonat magyar nyelvű fordítása: Áttekintés: OECD Irányelvek a magánélet védelméről és a személyes adatok határokon átvitelő áramlásáról (a továbbiakban: OECD-irányelvek)

⁹⁰ JÓRI András: *Az adatvédelmi jog generációi és egy második generációs szabályozás részletes elemzése*. PhD-dolgozat. Pécs, 2009. 29. <https://ajk.pte.hu/files/file/doktori-iskola/jori-andras/jori-andras-vedes-ertekezes.pdf> (letöltés: 2022. 03. 04.)

módosíthatni;⁹¹ mindezek a GDPR érintetti jogai közül a hozzáférési jogot, a helyesbítéshez való jogot és a törléshez való jogot előlegezik. Az OECD-irányelveket 2013-ban felülvizsgálták és modernizálták.⁹²

1981 – a máig hatályos 108. számú egyezmény

Míg az imént említett dokumentumok nem bírnak kötelező erővel, addig az Európa Tanács által elfogadott, a személyes adatok gépi feldolgozása során az egyének védelméről szóló 108. számú egyezmény⁹³ az első, jogilag kötelező erejű nemzetközi okmány az adatvédelem területén. Hatálya a személyes adatok gépi feldolgozása során a személyes adatok automatizált állományaira terjed ki, valamint a részes államok nyilatkozata alapján a nem gépi eszközökkel feldolgozott állományaira is, mindkét esetben a köz- és a magánszektorra vonatkozóan is.⁹⁴ Az EEEJ-hez és az OECD-irányelvekhez egyaránt kapcsolódik. Előbbivel a célja kapcsolja össze: a gépi személyesadat-feldolgozás során is minden egyén számára „biztosítva legyen, hogy jogait és alapvető szabadságjogait, különösen a magánélethez való jogát tiszteletben tartsák.”⁹⁵ Az OECD-irányelvekkel való kapcsolata abból ered, hogy egyértelműen merített annak rendelkezéseiből, főleg az adatok minősége és az adatalanyt védő garanciák tekintetében.⁹⁶ Új elem azonban a különleges adatokról rendelkezés, amely tiltja ezek gépi úton történő feldolgozását.⁹⁷ A 108. számú egyezmény a határokon átnyúló személyesadat-áramlás elősegítését szorgalmazza, ugyanakkor az egyezményt aláíró államok korlátozásokat is alkalmazhatnak az olyan országokba történő adattovábbításra vonatkozóan, ahol a védelem szintje alacsonyabb.⁹⁸

1983 – német alkotmánybíróági döntés

Az adatvédelemmel kapcsolatos felfogást gyökeresen megrengette a német alkotmánybíróság döntése, amely a népesség-, lakás-, foglalkozás- és munkahely-összeírást

⁹¹ OECD-irányelvek 7–14. pont

⁹² The OECD Privacy Framework

⁹³ Az egyének védelméről a személyes adatok gépi feldolgozása során, Strasbourgban, 1981. január 28. napján kelt egyezmény. Magyarországon kihirdette az 1998. évi VI. törvény (a továbbiakban: 108. számú egyezmény)

⁹⁴ 108. számú egyezmény 3. cikk 1–2. pont

⁹⁵ 108. számú egyezmény 1. cikk

⁹⁶ 108. számú egyezmény 5. és 8. cikk

⁹⁷ 108. számú egyezmény 6. cikk

⁹⁸ 108. számú egyezmény 12. cikk (3) bekezdés. A harmadik országokba irányuló, határokon átnyúló adatáramlás tekintetében megállapítja, hogy az adatok csak akkor továbbíthatók, ha a címzett állam vagy nemzetközi szervezet megfelelő szintű védelmet tud biztosítani magának. Kiegészítő jegyzőkönyv az egyének védelméről a személyes adatok automatikus feldolgozása során, a felügyeleti hatóságokról és a határokon átnyúló adatáramlásról szóló egyezményhez (2004. 01. 07.)

célzó 1983. évi népszámlálási törvény 9. § (1)–(3) bekezdéseit az Alaptörvényük alapján semmisnek nyilvánította.⁹⁹ Az indoklás szerint az említett bekezdések – amelyek alapján a statisztikai hivatalok a nevek kivételével egyedi adatokat továbbíthatnak más hatóságoknak anyakönyvi nyilvántartásokkal összevetés és ez utóbbiak javítása céljából – sértik az általános személyiségi jogot.¹⁰⁰ Az általános személyiségi jog felöleli az önrendelkezést is, amely alapján az egyén maga döntheti el, „hogyan nyilvánosságra hozza-e személyes életének egyes aspektusait, és ha igen, milyen mértékben.” A kockázatok abból fakadnak, hogy az automatikus adatfeldolgozással az egyén személyes vagy anyagi körülményeire vonatkozó konkrét információk korlátlan ideig tárolhatók és visszakereshetők, valamint összevethetők más forrásból származó adatokkal, és ezáltal teljes személyiségprofilok állíthatók össze. A népszámlálások statisztikai alapú jellege és sokrétű felhasználásának¹⁰¹ szükségessége nem teszi lehetővé, hogy célhoz kössék az adatgyűjtést, ezért az adatszolgáltatásra kötelezett állampolgárok személyiségi jogainak védelme, információs önrendelkezési jogának biztosítása érdekében az ilyen adatgyűjtéshez és -feldolgozáshoz külön követelményként kell meghatározni az anonimizálást, és az adatokat mindaddig bizalmasan kell kezelni, amíg azok egyéneknek tulajdoníthatók.¹⁰²

A német alkotmánybíróság döntése nemcsak abban az értelemben hatott az adatvédelmi jog alakulására, hogy számtalan országban jogszabály-módosításokhoz vezetett, hanem abban is, hogy – mivel az általános személyiségi jogból vezette le az információs önrendelkezési jogot, ami bekerült az európai adatvédelmi közgondolkodás áramába¹⁰³ – előtérbe került az a szemlélet, hogy az adatvédelemben a személyek védelme az elsődleges; emiatt az adatvédelmi jogszabályok generációs fejlődésében mindenképpen korszakhatárt jelent. Ezzel párhuzamosan a következő bő évtizedben a személyi számítógépek, az internetes kereskedelem stb. általános elterjedése az adatvédelem eme új megközelítését kívánta és igazolta is egyben.

⁹⁹ BVerfG. Az Első Szenátus 1983. december 15-i végzése - 1 BvR 209/83 - 1. pont. 213. (a továbbiakban: BVerfG. BvR 209/83.)

¹⁰⁰ BVerfG. BvR 209/83. 47–48. és Fejjegyzetek 5. pont

¹⁰¹ A népszámlálások adatai nem csak tisztességes célokra hasznosíthatók. A washingtoni Holokauszt Múzeumban található lyukkártya-osztályozó berendezés felirata szerint az IBM szervezte meg az 1933-as németországi népszámlálást. A dátum arra enged következtetni, hogy a cél a zsidóság összeszámlálása és azonosítása volt. GALÁNTAI Zoltán: *E-privacy olvasókönyv. Dialógusok a privacyről és az internetről – meg a cyberpornóról, a megfigyelésekről és egyebekről.* <https://mek.oszk.hu/04100/04134/html/#7> (letöltés: 2022. 03. 06.)

¹⁰² BVerfG. BvR 209/83. 144–162.

¹⁰³ JÓRI i. m. 16–27.

1995 – az adatvédelmi irányelv¹⁰⁴

Bár az Európai Bizottság abban bízott, hogy a 108. számú egyezmény „megoldja majd az uniós harmonizáció kérdését,”¹⁰⁵ azonban a nemzeti adatvédelmi jogszabályok sokféleségéből eredő eltérő védelmi szint; valamint az, hogy az említett egyezményben foglalt elveket kiegészítse és tartalmat adjon nekik, megkövetelte a tagállami jogszabályok összehangolását.¹⁰⁶ A többéves előkészítő munka során az is „nyilvánvalóvá vált, hogy a tagállamok erősen megosztottak az adatvédelmi szabályozás kérdésében,”¹⁰⁷ de végül 1995-ben elfogadták az egyének védelméről és az ilyen adatok szabad áramlásáról szóló irányelvet, amely több mint húsz éven keresztül az uniós adatvédelem meghatározó dokumentuma lett.

Az adatvédelmi irányelv – az egyének védelme a személyes adataik feldolgozása tekintetében – a 108. számú egyezmény megerősítését és kiegészítését szolgálja. Erre vonatkozóan „Az adatfeldolgozás jogszerűvé tételére vonatkozó kritériumok” cím alatt az adatfeldolgozás jogalapjai, valamint „Az érintett tájékoztatása” cím alatt a kapcsolódó tájékoztatási kötelezettségek találhatók, ezekről a tagállamoknak kellett rendelkezniük. Szintén szerepelt már a 108. számú egyezményben a különleges adatok kezelése, amelyre vonatkozóan az adatvédelmi irányelv megengedi a tagállamok számára tilalom felállítását, de tételesen sorolja föl azokat az eseteket, amelyekben a tilalom nem alkalmazható.¹⁰⁸

Új elemként jelentek meg az automatizált egyedi döntések, amelyek felhasználását az érintettek védelme érdekében korlátozza, vagy használatára garanciákat biztosít,¹⁰⁹ ami azért fontos, mert a számítógép által létrehozott profil a szubjektív elemeket nem veszi figyelembe, ami például hitelbírálatnál vagy munkahelyi előmenetelnél hátrányosan befolyásolhatja a döntést. Szintén új elem az érintett részére az adatkezelés vagy adattovábbítás elleni tiltakozási jog biztosítása, például az adatkezelői előrejelzést követően a személyes adatok közvetlen üzletszerzési célú feldolgozására vonatkozóan.¹¹⁰ Ez utóbbi azért különösen fontos, mert az adatvédelmi irányelv „nem akadályozza a tagállamokat a területükön tartózkodó fogyasztókat célzó marketingtevékenységek szabályozásában.”¹¹¹ Az adatvédelmi irányelv hozta létre a

¹⁰⁴ 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 (a továbbiakban: adatvédelmi irányelv)

¹⁰⁵ JÓRI i. m. 31.

¹⁰⁶ Adatvédelmi irányelv (8)–(11) preambulumbekkezdés

¹⁰⁷ JÓRI i. m. 31. hivatkozik a következő forrásra: Rosemary JAY – Angus HAMILTON: *Data Protection Law and Practice*. Sweet and Maxwell, London, 1999. 9–10.

¹⁰⁸ Adatvédelmi irányelv 8. cikk

¹⁰⁹ Adatvédelmi irányelv 15. cikk

¹¹⁰ Adatvédelmi irányelv 14. cikk

¹¹¹ Adatvédelmi irányelv (71) preambulumbekkezdés

személyesadat-feldolgozás vonatkozásában a tanácsadói státuszban működő és függetlenül eljáró 29. cikk szerinti munkacsoportot, amely az egységes értelmezést segítő munkaanyagokat állított össze, véleményt nyilvánított stb. A tagállamoknak pedig független felügyeleti hatóságról kellett gondoskodni.¹¹²

Az EU alapvető célja a személyek, áruk, szolgáltatások és a tőke szabad áramlásán alapuló egységes belső piac létrehozása, e cél az adatvédelmi irányelvnek már a címében megjelenik. Személyes adatok tagállamok közötti továbbításában korlátozásokat – tekintve, hogy maga az irányelv hárítja el a védelmi szint különbségeit – nem enged; harmadik országokba azonban megfelelő védelmi szinthez köti az adattovábbítást, amelynek megítélési szempontjait is megadja. Ezen túlmenően felsorolja azokat a feltételeket is, amelyek a nem megfelelő védelmi szint esetében is lehetővé teszik adott országba az adatátadást (pl. szerződéses biztosítékok), s csupán azon harmadik országokba irányuló adattovábbítást tiltja, amelyek esetében a Bizottság vizsgálata nem megfelelő védelmi szintet állapított meg.¹¹³

Az adatvédelmi irányelv a kettős célkitűzését – az egyének védelme és az ilyen adatok szabad áramlása – húszéves hatálya alatt sem tudta maradéktalanul megvalósítani. Ennek oka magával az irányelv jogszabálytípusával is magyarázható: az elérendő szabályozási elveket és rendelkezéseket a tagállamok eltérő módon, a nemzeti sajátosságaik figyelembevételével ültethették át a saját jogrendszerükbe.¹¹⁴ Az eltérő szintű adatvédelem gátjává vált a személyes adatok szabad áramlásának, és oda vezetett, hogy éppen az adatvagyonok megalapozása idején, az online platformok megerősödése idején Európában nem tudtak kialakulni adatvezérelt techcégek, ami a későbbiekben a piaci versenyt is hátrányosan befolyásolta.

2000 – a személyes adatok védelméhez fűződő jog mint alapjog

Az Európai Tanács javaslatára egyetlen dokumentum, Az Európai Unió Alapjogi Chartája foglalja össze, és ezáltal meg is erősíti az alapvető jogokat és szabadságokat.¹¹⁵ A Chartába harmadik generációs jogok is bekerültek, köztük önállóan nevesítve a személyes adatok védelméhez fűződő jog: „Mindenkinek joga van a rá vonatkozó személyes adatok védelméhez. Az ilyen adatokat csak tisztességesen és jóhiszeműen, meghatározott célokra, az érintett személy hozzájárulása alapján vagy valamilyen más, a törvényben rögzített jogos okból lehet kezelni. Mindenkinek joga van ahhoz, hogy a róla gyűjtött adatokat megismerje, és joga

¹¹² Adatvédelmi irányelv 28. cikk

¹¹³ Adatvédelmi irányelv 25–26. cikk és (57) preambulumbekkezdés

¹¹⁴ Az adatvédelmi irányelv Magyarországon az Infotv.-be került átültetésre.

¹¹⁵ Az Európai Unió alapjogi chartája (a továbbiakban: Charta) preambuluma

van azokat kijavíttatni.”¹¹⁶ A Chartát 2000-ben a nizzai csúcstalálkozón hirdette ki ünnepélyesen a Parlament, a Tanács és a Bizottság. Kötelező erővel az európai alkotmány tervezetének elfogadása ruházta volna fel, de a ratifikációs folyamat elbukott, s majd csak a lisszaboni szerződés elfogadása tette jogilag kötelező erejűvé: „az Unió elismeri az Európai Unió Alapjogi Chartájának [...] szövegében foglalt jogokat, szabadságokat és elveket; e Charta ugyanolyan jogi kötőerővel bír, mint a Szerződések.”¹¹⁷ Ez azt jelenti, hogy a Charta az elsődleges joganyag része lett, ezáltal az is vizsgálándó szempont lett, hogy a másodlagos joganyag és az ebből következő nemzeti jogszabályi intézkedések megfelelnek-e a Charta rendelkezéseinek.

Ezt vizsgálta az EUB írországi és osztrák bíróságok által előterjesztett előzetes döntéshozatali kérelmek alapján.¹¹⁸ A távközlési adatok megőrzése hatékony nyomozati eszköz a bűnüldözés, különösen a szervezett bűnözés és a terrorizmus felderítése során, szükséges, hogy a bűnüldöző szervek ezen adatokhoz hozzáférjenek, ezért került elfogadásra a 2006/24/EK irányelv,¹¹⁹ mely a hírközlési szolgáltatók által előállított vagy kezelt adatok megőrzésére vonatkozó kötelezettségről rendelkezik. Az EUB az említett irányelv összeegyeztethetőségét vizsgálta a Charta 7. és 8. cikkében foglalt, a magánélet tiszteletben tartásához való és a személyes adatok védelméhez való joggal, továbbá az ezekbe való beavatkozás arányosságát. A 2006/24/EK irányelv hosszú időre különböző adatfajták nagy tömegének tárolását teszi lehetővé korlátlan számú személy tekintetében, akik szinte kizárólag olyan személyek, akiknek a magatartása nem szolgált okot az őket érintő adatok megőrzésére, ami által a hatóságok a magánéletükről információkat szerezhetnek, és ezen adatokat különböző célokra használhatják fel. Az EUB aránytalannak minősítette – a magánülethez és a személyes adatok védelméhez való joggal összefüggésben – az adatmegőrzési kötelezettséget. Mivel a jogalkotó nem tartotta tiszteletben az arányosság elvének követelményeit, az EUB a 2006/24/EK irányelvet érvénytelennek nyilvánította.¹²⁰

¹¹⁶ Charta 8. cikk

¹¹⁷ Lisszaboni szerződés. Az Európai Unióról szóló szerződés és Az Európai Közösséget létrehozó szerződés módosításáról (a továbbiakban: lisszaboni szerződés) 6. cikk (1) bekezdés

¹¹⁸ ECLI:EU:C:2014:238. A Bíróság ítélete (nagytanács) a C-293/12. és C-594/12. sz. egyesített ügyekben (2006/24/EK irányelv érvényessége) 2014. április 8. (a továbbiakban a lábjegyzetekben: EUB-ítélet C-293/12. és C-594/12. sz. ügyek)

¹¹⁹ Az Európai Parlament és a Tanács 2006/24/EK irányelve (2006. március 15.) a nyilvánosan elérhető elektronikus hírközlési szolgáltatások nyújtása, illetve a nyilvános hírközlő hálózatok szolgáltatása keretében előállított vagy feldolgozott adatok megőrzéséről és a 2002/58/EK irányelv módosításáról. Hatályos 2006. 05. 03-ig. (a továbbiakban: 2006/24/EK irányelv)

¹²⁰ EUB-ítélet C-293/12. és C-594/12. sz. ügyek 17–73. pontok

2016-tól – az EU adatvédelmi reformja

„Az a tény, hogy a személyes adatok kezelése tekintetében a természetes személyek jogai és szabadságai egyes tagállamokban eltérő szintű védelmet élveznek, különösen, ami a személyes adatok védelméhez való jogot illeti, a személyes adatok Unióban történő szabad áramlásának útjában állhat. Ebből eredően ezek az eltérések [...] torzíthatják a versenyt.”¹²¹ A piaci verseny szempontjából a technológiai fejlődés, a felhasználókról folyamatosan képződött nagy adatmennyiség és a digitális óriásvállalatok is kihívást jelentettek, és jelentenek ma is. A tagállami átültetésből eredő széttagoltság megszüntetése végett, valamint a verseny előmozdítása érdekében – a big data jelenséget továbbra is „jogérvényesítési, ellenőrzési, betartatási, kikényszerítési problémának”¹²² tekintve – az EU a jog eszközeivel válaszolt, és az adatvédelmi szabályok átfogó reformját javasolta. Ennek első lépéseként az irányelvi szabályozás helyett a rendeleti szintű szabályozás mellett döntött, és négyéves rendes jogalkotási eljárást követően, 2016. május 24-én hatályba lépett a GDPR, amelyet 2018. május 25-étől kötelezően és közvetlenül kell alkalmazni.

Az EU adatvédelmi reformjának jogi eszköze a bűnügyi adatvédelmi irányelv,¹²³ valamint a természetes személyeknek az uniós intézmények által kezelt személyes adatait érintő rendelkezések,¹²⁴ ezek azonban nem tartoznak vizsgálódásom körébe, a teljesség igénye végett utaltam rájuk. Az általános szabályokat rögzítő GDPR-al összhangba kell hozni a speciális területeket érintő szektorális jogszabályokat is, így a hozzá szorosan kapcsolódó elektronikus hírközlési adatvédelmi jogszabályokat, ezért az EU e területre vonatkozóan is a rendeleti szabályozás mellett döntött, és 2017-re elkészült az e-Privacy rendelet tervezete. Tervek szerint 2018. májustól kellett volna alkalmazni, párhuzamosan a GDPR-al, azonban a 2025. év elején visszavonásra került.¹²⁵ Ebből következően jelenleg és a közeljövőben az elektronikus hírközlési adatvédelmi irányelv hatályos.

¹²¹ GDPR 9. preambulumbekkezdés

¹²² ZÖDI Zsolt: *Privacy és a Big Data*. Fundamentum 2017/1–2. 27. <http://fundamentum.hu/sites/default/files/fundamentum-17-1-2-02.pdf> (letöltés: 2019. 01. 14.)

¹²³ 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 szóló, 2016. április 27-i (EU) 2016/680 európai parlamenti és tanácsi irányelv. Magyarországon – a 2018. július 26-án kelt módosítással – implementálta a 2011. évi CXII. törvény az információs önrendelkezési jogról és az információszabadságról (a továbbiakban: Infotv.).

¹²⁴ Az Európai Parlament és a Tanács (EU) 2018/1725. rendelete (2018. október 23.) a természetes személyeknek a személyes adatok uniós intézmények, szervek, hivatalok és ügynökségek általi kezelése tekintetében való védelméről és az ilyen adatok szabad áramlásáról, valamint a 45/2001/EK rendelet és az 1247/2002/EK határozat hatályon kívül helyezéséről

¹²⁵ COM(2025) 45 final. Mellékletek 28.

3. Alapfogalmak

3.1. Az adatvédelem

„Az adatvédelem – Jóri András megfogalmazása szerint – olyan jogi védelem, amely az egyének magánszférájának védelmét célozza az egyénnel kapcsolatba hozható adatok (személyes adatok) kezelésére vonatkozó szabályok előírásával.”¹²⁶ E definícióból az adatvédelemnek három eleme azonosítható: a tárgya, a célja és a módszere. Eszerint a tárgya a személyes adat; célja tekintetében elengedhetetlen hangsúlyozni, hogy nevével ellentétben nem az adatokat védi, hanem a személyeket;¹²⁷ és ezt oly módon teszi, hogy szabályokat ír elő az egyénnel kapcsolatba hozható adatok kezelésére vonatkozóan.¹²⁸ Fontos mindehhez hozzátenni azt is, hogy a jogi védelem tartalma a fogalom megjelenése óta többször jelentősen változott, és jelenleg is változásban van.¹²⁹

Az adatvédelem történetének áttekintése kidomborította annak mozgatórugóit, láttatta a szabályozás folyamatának alakulását. Anélkül, hogy állást foglalnánk az adatvédelmi szabályozás generációs határai kérdésében, annyit mindenképpen érdemes rögzíteni, hogy három fogalom kikristályosodása és dominanciája figyelhető meg. A 20. század derekának nemzetközi dokumentumaiban, az EJENY-ben és az EJEE-ben a magánélet, magánszféra védelme játszott hangsúlyos szerepet, az ehhez való jogot fektették le, s ebbe érthető bele, ebből nő ki az adatvédelem. Ez a magyarázata annak, hogy az adatvédelem nem az adatok védelmét jelenti, hanem a személyek védelmét az adataik kezelése tekintetében. Az 1980-as évek elején az OECD-irányelvekben és a 108. számú egyezményben nevesítésre kerültek a személyes adatok, valamint ezekkel kapcsolatban az adatkezelési elvek és az érintetti jogok. Innen már csak egy lépés volt, hogy 1983-ban a német alkotmánybíróság az általános személyiségi jogból levezette az információs önrendelkezési jogot. A magánélet védelme, a személyes adatok és az információs önrendelkezési jog pillanatok alatt megmozgatta az adatvédelem vérkeringését, nélkülük a modern adatvédelmi jog elképzelhetetlen. A továbbiakban e fogalmakat tekintem át.

¹²⁶ JÓRI i. m. 19.

¹²⁷ MAJTÉNYI László: *Információs jogok*. In: HALMAI Gábor – TÓTH Gábor Attila (szerk.): *Emberi jogok*. Bp., Osiris, 2003. 579.

¹²⁸ Az adatvédelem fogalmát más definíciók is lényegében e három elem mentén határozzák meg: „Az adatok kezelésével kapcsolatos törvényi szintű jogi szabályozás formája, amely az adatok valamilyen szintű, előre meghatározott csoportjára vonatkozó adatkezelés során érintett személyek jogi védelmére és a kezelés során felmerülő eljárások jogszerűségeire is vonatkozik.” ITB 8. sz. ajánlása, idézi BALOG Zsolt György: *A személyes adatok védelme és a közérdekű adatok nyilvánossága*. Előadásmásolat 2. dia. <https://slideplayer.hu/slide/2150301/> (letöltés: 2023. 01. 02.); „A személyes adatok jogszerű kezelését, az érintett személyek védelmét biztosító alapelvek, szabályok, eljárások, adatkezelési eszközök és módszerek összessége.” NAIH: Adatvédelmi értelmező szótár. <https://www.naih.hu/adatvedelmi-szotar> (letöltés: 2023. 01. 01.)

¹²⁹ JÓRI i. m. 16.

3.2. A magánélet

Az USA-ban a védelem tárgya a privacy, amit a magánélet, magánszféra szóval szokás fordítani, de jelentése sokkal tágabb és összetettebb attól. A privacy védelmét Warren és Brandeis tanulmánya – a bírói esetjog nyomán – még csak az „egyedül hagyatáshoz való jog”-ként aposztrofálta,¹³⁰ és a képmásnak és a jó hírnévnek a védelmére utalt vele, de az „idők folyamán az »általános személyiségi jog« megfelelője lett.”¹³¹ Lényegében hasonlóan látja Jóri is: „a privacy nemcsak a magánszféra, hanem a tágabb értelemben vett autonómia védelmét jelenti;” ill. „mára az általános személyiségi jog megfelelőjeként értékelhető.”¹³² Az amerikai jogrendszerben a privacy védelme tehát a személyes döntési szabadság védelméhez kötődik.¹³³ Ezt erősíti Szabó Máté Dániel privacy-definíciója is: „az egyén joga ahhoz, hogy magáról döntsön.”¹³⁴ Az európai dokumentumok (EJEE, Charta) a magán- és családi élet, a lakás/otthon és a levelezés/kapcsolattartás tiszteletben tartását hangsúlyozzák, és a magánszféra védelmét az emberi méltóság védelméhez kötik.¹³⁵

Az alapjogokhoz kapcsolódást lehetővé tévő megfontolások nem visznek előbbre a magánélet jelentésének feltárásában, ezért a kutatók a kiterjedésének meghatározásával, a dimenzióinak feltérképezésével igyekeznek megközelíteni a problémát. Kiemelkedő erre vonatkozóan az a projekt, melyben kilenc ország kutatói – a magánélet alkotmányos védelmét és a szakirodalmat alapul véve – közösen vizsgálták a magánélet kiterjedését, és nyolc típust azonosítottak: a testi, térbeli, kommunikációs, reputációs, intellektuális, döntési, valahová tartozási és viselkedési szférát. Ezeket a személyestől a nyilvánosig terjedő, összesen négy zóna mentén is rendszerezték, továbbá egy kétdimenziós modellben is strukturálták a szabadság két aspektusa mentén. Az egyik dimenzióba kerültek azok a típusok, amelyekben a valamtől való szabadság jelenik meg, a másik dimenzióba pedig azok, amelyekben a valamihez való szabadság realizálódik, tulajdonképpen az információs önrendelkezés. Megállapították továbbá, hogy mindegyiket átszövi, mindegyikkel érintkezik az információs magánszféra, vagyis mindegyik típusnak van információs szegmense. Például a testi magánszféra nem

¹³⁰ WARREN–BRANDEIS i. m. 8.

¹³¹ SÓLYOM László: *A személyiségi jogok elmélete*. Bp., Közgazdasági és Jogi Könyvkiadó, 1983. 29. Ehhez az is hozzátartozik, hogy az USA-ban pl. a személyes adat nyilvánosságra hozatala kapcsán nem a publikált adat bizalmas vagy személyes jellege határozza meg a védelem határait, hanem a nyilvánosságot megengedő különböző privilégiumok, vagyis a privacy–sajtószabadság szembenállása. Uo. 322.

¹³² JÓRI i. m. 13–15.

¹³³ MENYHÁRD Attila: *A magánélethez való jog elméleti alapjai*. In *Medias Res* 2014/2. 385.

¹³⁴ SZABÓ Máté Dániel: *Kísérlet a Privacy fogalmának meghatározására a magyar jogrendszer fogalmaival*. *Információs Társadalom* 2005/2. 46.

¹³⁵ MENYHÁRD (2014) i. m. 385. A személyiségi jogokat Magyarországon is az emberi méltóságból vezetik le, pl. a Ptk. (2:42. § (2) bekezdés).

csupán a fizikai távolságban ragadható meg, hanem a testtel kapcsolatos információk szálat is magában foglalja, tehát az egészségügyi vagy genetikai információkat is, és a védelemnek ezekre is ki kell terjednie, csakúgy, mint bármelyik típus esetén.¹³⁶ (Az 1. melléklet tartalmazza A magánélet tipológiája című ábrát.)

Dolgozatom témája szempontjából természetesen a személyes adatok védelmének van jelentősebb szerepe, pontosabban a személyek védelmének a személyes adataik kezelése kapcsán. A személyes adatok nem megfelelő kezelése azonban gyakran hordoz kockázatokat a magánéletre vonatkozóan. Ennek oka az, hogy tárgyuk szerint többszörösen átszövik egymást, érintkezési pontok vannak közöttük: a magánszféra védelmének előbb említett elemei az otthon, családi élet, levelezés, fizikai integritás stb.; ugyanakkor személyes adat lehet bármilyen adat, ami összefügg az azonosított vagy azonosítható személlyel.

Itt jegyzem meg, hogy az adatvédelmi irányelv az egyének védelméről, a GDPR a természetes személyek védelméről szól; előbbi több mint egy tucatszor használja a magánélet fogalmát, utóbbi mindössze egyszer. Számomra ez is hangsúlyozza azt, hogy a GDPR már nem csak a magánszféra-védelem részeként létezik, hanem markánsan képviseli az adatvédelem önálló alapjoggá válását. A két fogalom elhatárolása a jogvédelem szempontjából különösen fontos. Adatvédelmi jogsértés esetén hatósági eljárás kezdődik, amelynek során az adatkezelőnek kell bizonyítania, hogy mindent szabályosan tett, ellenkező esetben a hatóság bírságot szabhat ki; a magánélet megsértése polgári peres úton (személyiségi jogi perben) orvosolható, ahol az áldozatnak kell bizonyítania a jogsértést, és az eljárás sérelemdíj megfizetésére kötelezéssel zárulhat.

A magánélet dimenzióinak tág köre és sokrétűsége olyan kérdéseket is felvet, amelyekről sokszor eszünkbe sem jut, hogy a jog által szabályozandók. A következő ügy elgondolkodtatja az olvasót az udvariasság, illem határainak feszegetése által a hagyományos értékrendek és a GDPR kapcsolatáról, a világunk által generált helyzetek és a jogi kontroll viszonyáról. Az EUB először foglalkozott, a francia államtanács előzetes döntéshozatali kérelme alapján, a megszólításra és nemi identitásra vonatkozó személyes adatok gyűjtésének, kezelésének gyakorlatával. Az ítélet indoklása szerint az, hogy a vasúttársaság ügyfeleinek a menetjegyek online értékesítési felületén az „úr” vagy „hölgy” megjelölés kiválasztásával kötelezően fel kell tüntetniük megszólításukat, sérti a GDPR adattakarékosság elvét; továbbá nem szükséges elem a kereskedelmi kommunikációban és nem szükséges a szerződés

¹³⁶ Bert-Jaap KOOPS – Bryce Clayton NEWELL – Tjerk TIMAN – Ivan ŠKORVÁNEK – Tomislav CHOKREVSKI – Maša GALIĆ: *A Typology of Privacy*. *University of Pennsylvania Journal of International Law* 38(2)/2017. 566–569. <https://scholarship.law.upenn.edu/cgi/viewcontent.cgi?article=1938&context=jil> (letöltés: 2023. 02. 02.)

teljesítéséhez; valamint az ügyfelek alapvető jogai és szabadságai, így a magánélet tiszteletben tartására vonatkozó jog – különösen a nemi identitáson alapuló hátrányos megkülönböztetés kockázata miatt – elsőbbséget élveznek a vasúttársaság által hivatkozott jogos érdekekkel, a tradicionális udvariassági szabályokkal szemben. A nemre vonatkozó adatok megadása csak az azonos nemű utasok számára elérhető hálókocsikba menetjegyet vásárló ügyfelektől követelhető meg.¹³⁷

3.3. Az információs önrendelkezési jog

Az információs önrendelkezési jogot a német alkotmánybíróság (1983. évi népszámlálási törvény) vezette le az általános személyiségi jogokból, s ebből az is következik, hogy nem lehet azonosítani az adatvédelemmel, hiszen attól egyrészt későbbi fejlemény, másrészt „a korai adatvédelmi törvények nem biztosítottak az egyénnek rendelkezési jogot személyes adatai felett.”¹³⁸ Jelentésének értelmezéséhez az önrendelkezésből kell kiindulni, amely alapján az adatalany, az érintett rendelkezik a saját személyes adatai felett, ő dönti el, hogy hozzájárul-e személyes adatai kezeléséhez, s ha igen, milyen mértékben, kéri-e a törlését, hordozását stb.; ezeket az érintetti jogok tartalmazzák a GDPR-ban.

A magyar jogalkotásban egyenes ívet követ az önrendelkezés joga. Már a személyes adatok védelméről és a közérdekű adatok nyilvánosságáról szóló 1992. évi LXIII. törvény célként fektette le, hogy „személyes adatával mindenki maga rendelkezzen,”¹³⁹ majd az Infotv. a címében is hordozza, hogy „az információs önrendelkezési jogról és az információszabadságról” rendelkezik.¹⁴⁰ Az Infotv. megoldása Európában is „egyedülálló,” mert az információszabadságot és az adatvédelmet egy törvény szabályozza,¹⁴¹ amely így nemcsak védelmet nyújt az érintettek számára a személyes adataik kezelése tekintetében, hanem mintegy egyensúlyt teremtve, ezzel párhuzamosan az érintettek számára tevékeny közreműködést, önrendelkezési jogot is biztosít.¹⁴²

¹³⁷ ECLI:EU:C:2025:2. A Bíróság ítélete (első tanács) a C-394/23. sz. ügyben (a megszólításra vonatkozó adatok), 2025. január 9. 13–19., 41–42. és 71. pont

¹³⁸ JÓRI i. m. 16–17.

¹³⁹ 1992. évi LXIII. törvény a személyes adatok védelméről és a közérdekű adatok nyilvánosságáról 1. § (1) bekezdés

¹⁴⁰ Az információszabadság (freedom of information, FOI) „azoknak a jogintézményeknek az összefoglaló neve, amelyek a mai viszonyok között akarnak valódi esélyt adni a vélemény- és sajtószabadságnak, valamint a polgárok »informált részvételének« a társadalom ügyeiben, és ezért az államapparátus információit nyilvánossá teszik.” SÓLYOM László: *Egy új szabadságjog: az információszabadság*. Valóság 1988/9. 14.

¹⁴¹ PÉTERFALVI Attila: *Az adatvédelem fejlődésének történeti áttekintése Magyarországon a GDPR hatálybalépéséig*. In: PÉTERFALVI Attila (szerk.): *Személyes adatok az információs jogok felügyeletének elmúlt 25 évéből*. Bp., NAIH, 2020. 42.

¹⁴² Infotv. preambuluma

3.4. A személyes adat

Az adatvédelem központi eleme a személyes adat, definiálása nélkülözhetetlen támasz a jogalkalmazók számára, de az adatalanyok számára is elengedhetetlen segítség, ha tisztában akarnak lenni azzal, hogy egy-egy szervezet vagy szolgáltató adatkezelése jogszerűen valósul-e meg. A személyes adat a GDPR alapján az azonosított vagy azonosítható természetes személyre – e rendelet alkalmazásában: érintetre – vonatkozó bármely információ; „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.”¹⁴³ A preambulumban az online azonosítók között nevesíti az IP-címeket és a cookie-azonosítókat,¹⁴⁴ mint az interneten hagyott nyomokkal történő azonosítás példáit. Az adatvédelmi irányelv ezeket még nem tartalmazta, a jogalkotók által a GDPR-ban kiemelt példák a technológiai fejlődés követésére utalnak. Az adattípus korunkban betöltött szerepe miatt a genetikai adat új elemként került be a GDPR személyesadat-fogalmába.

Annak értékeléséhez, hogy egy adat személyes adat-e, a fenti meghatározás kulcsszavai alapján négy elemet szükséges vizsgálni, amelyek értelmezéséhez a 29. cikk alapján létrehozott adatvédelmi munkacsoport vonatkozó véleményére támaszkodom.¹⁴⁵ Definiálni kell a négy elem egyikeként a természetes személy fogalmát, amihez az EJENY és a tagállamok pontosabb meghatározása, így a Ptk. adnak támpontot. Ezek alapján a jogképes élő személyek tekintendők természetes személynek,¹⁴⁶ amiből az is következik, hogy sem az elhunytak, sem a jogi személyek nem tartoznak a természetes személyek körébe. Az elhunytakra vonatkozó információk utalhatnak élő személyekre is, ezért a GDPR a tagállamok hatáskörébe helyezi az elhunytak személyes adatai kezelésének szabályozását.¹⁴⁷

A négy elem közül a „bármely információ” kifejezés a személyes adat fogalmának – a jogalkalmazói szándék szerinti – tág értelmezésére ad lehetőséget. Az információ szó jelentésének vonatkozásában nem találunk definíciót, és figyelembe véve a „bármely” jelzót, a

¹⁴³ GDPR 4. cikk 1. pont

¹⁴⁴ GDPR (30) preambulumbekzdés

¹⁴⁵ WP136. A 29. cikk alapján létrehozott adatvédelmi munkacsoport: 4/2007 vélemény a személyes adat fogalmáról. (A személyes adat fogalmát az adatvédelmi irányelv alapján értelmezi, de mivel a definíció a GDPR-ban lényegében nem változott, megállapításai továbbra is helytállóak.)

¹⁴⁶ Az EJENY 6. cikke szerint „mindenkinek joga van ahhoz, hogy jogalanyiságát mindenhol elismerjék.” A jogalanyiség összetevői közül alapvetően a jogképességet (Ptk. 2:1.–2:4. §) kell vizsgálni, mely a fogamzás időpontjától (feltétele az élve születés, tehát a születésig a jogképesség függő helyzetben van) a halálig tart.

¹⁴⁷ GDPR (27) preambulumbekzdés. Magyarországon az Infotv. 25 §-a rendelkezik az elhunytak személyes adatai kezelésének szabályairól.

szónak az általános jelentéséből is kiindulhatunk ('értesülés, hír, üzenet, tájékoztatás'), a 29. cikk alapján létrehozott adatvédelmi munkacsoport tulajdonképpen a személyre vonatkozó állításnak tekinti, és három szempont szerint csoportosítja. Az információ természete alapján objektív vagy szubjektív lehet. Az utóbbi akár azt is megengedi, hogy az információ hamis legyen, ezért biztosít a GDPR az érintett részére hozzáférési, helyesbítési és törlési jogot.¹⁴⁸ Tartalma szerint gyakorlatilag bármihez kötődhet: a magánélethez, a családhoz, munkához, társas léthez, gazdasági tevékenységhez, biológiai jellemzőkhöz stb. Formáját tekintve: szöveges, számszerű, képi, akusztikus stb. formát ölthet, és a kapcsolódó adathordozó is rendkívül változatos lehet, papír, kód, DVD stb.

A harmadik elem a „vonatkozó” szó, ami az előbb említett információ és a természetes személy kapcsolatát jelenti, és ami a tartalomban, a célban vagy az eredményben érhető tetten. A fotó tartalomelemként vonatkozik a személyre; a takarító személyzet által az irodai vezetékes telefonról indított hívás jelzi a munka befejezési időpontját, ezáltal célelemként vonatkozik a személyre; ha a taxitársaság helyzetmeghatározást alkalmaz, az eredményelem, mert a rendelési helyhez legközelebb tartózkodó autót tudja az utasért küldeni. A célelem és az eredményelem kiemeli és egyben előre is vetíti a profilalkotásban való felhasználás jelentőségét.

Negyedik elemként vizsgálandó annak jelentése, hogy az információ „azonosított vagy azonosítható” természetes személyre vonatkozik. A természetes személy közvetlenül azonosítottnak tekinthető a neve által például egy orvosi váróteremben, de a település lakosai közül a név mellett a születési idő és/vagy lakcím által közvetve lesz azonosítható, ez utóbbiak különböztetik meg a többi azonos nevű személytől. Az azonosítást az azonosítóknak nevezett különleges információk teszik lehetővé, amelyek összefüggésben, szoros kapcsolatban vannak az adott egyénnel (név, szám, helymeghatározó adat stb.). Az, hogy ezek közül akár „több tényező”¹⁴⁹ is szóba jöhet, arra utal, hogy az információk összekapcsolhatók, így segítve az azonosítást. A felsorolt azonosítók esetében egyértelmű az azonosíthatóság, de a gazdasági élet dinamikus változása mindig felszínre hoz olyan jellemzőket, amelyeket a jogalkotók tényszerűen példaként nem soroltak fel, a GDPR azonban ezeknek a tekintetében is eligazít. Ezt szemlélteti a következő jogeset.

A gépjárműalkatrészek nagykereskedelmével foglalkozó német vállalkozások szakmai szervezete és a Scania svéd járműgyártó közötti jogvitában¹⁵⁰ eljáró bíróság előzetes

¹⁴⁸ GDPR 15–17. cikk

¹⁴⁹ GDPR 4. cikk 1. pont

¹⁵⁰ A jogvita tárgya – a járműjavítási és -karbantartási információknak a Scania általi rendelkezésre bocsátása – a gazdasági verseny szempontjából bír jelentőséggel.

döntéshozatal iránti kérelmet terjesztett elő, és többek között arra várt választ az EUB-tól, hogy a járműazonosító szám, az ún. VIN személyes adatnak minősül-e. Az EUB döntése szerint a VIN alapvetően nem személyes adat, és különösen nem az, ha a jármű, amelyre a VIN-t kiadták, nem természetes személyé; ugyanakkor a „gazdasági szereplők valószínűsíthetően rendelkeznek olyan módszerekkel, amelyek lehetővé teszik számukra, hogy valamely VIN-t azonosított vagy azonosítható természetes személyhez társítsanak,” ebből következően a VIN az ő számukra személyes adatnak minősül.¹⁵¹ Mivel egy adat nem feltétlenül önmagában teszi azonosíthatóvá a természetes személyt, ezért a GDPR előírja, hogy az azonosíthatóság meghatározásakor „minden olyan módszert figyelembe kell venni – ideértve például a megjelölést –, amelyről észszerűen feltételezhető, hogy az adatkezelő vagy más személy a természetes személy közvetlen vagy közvetett azonosítására felhasználhatja,” mindez az objektív tényezők, így a költségek, időigény és a technológia függvénye.¹⁵² A 29. cikk alapján létrehozott adatvédelmi munkacsoport megerősíti ezt: minden olyan módszerrel számolni kell, „amit az adatkezelő vagy más személy valószínűleg felhasználna az említett személy azonosítására.”¹⁵³ A „felhasználna” fordulat egyúttal arra is utal, hogy maga az azonosíthatóságra való képesség a fontos.¹⁵⁴ Ebből következően, ha a kérdést előterjesztő bíróság a vizsgálata során megállapítja, hogy a VIN-t személyes adatnak kell tekinteni, akkor ez a járműgyártók számára azt jelenti, hogy az általuk gyártott járművek VIN-jét a független gazdasági szereplőknek mint adatkezelőknek a rendelkezésére kell bocsátaniuk.¹⁵⁵ A jogeset arra mutat rá, hogy a GDPR fogalommeghatározása lehetővé teszi a személyes adat tág, kiterjesztő értelmezését, és korunk digitális környezete miatt nem lehet messze az az idő, amikor minden információ személyes adatként fogható fel, ezzel együtt a GDPR hatálya alá is kerül. Az adatok dömpingszerűen, mértéktelenül személyessé válása oda vezethet, hogy az adatvédelem „kötelezettségrendszer nem tartható fenn érdemi módon,” megoldásként „a megfelelési kötelezettségek intenzitásának csökkentése” vagy „a személyes adatok szűkebb értelmezése” is szóba jöhet.¹⁵⁶ Éppen ez utóbbira, a személyes adatok szűkítő meghatározására

¹⁵¹ ECLI:EU:C:2023:837. A Bíróság ítélete (harmadik tanács) a C-319/22. sz. ügyben (alkatrész-kereskedők kontra Scania), 2023. november 9. 48–49. pont (a továbbiakban a lábjegyzetekben: EUB-ítélet C-319/22. sz. ügy)

¹⁵² GDPR (26) preambulumbekkezdés

¹⁵³ WP136. 23.

¹⁵⁴ PÓK László: *Egy kis lépés a személyes adat fogalmának relatív(abb) értelmezése felé?* Blogbejegyzés. 2023. november 15.

https://gdpr.blog.hu/2023/11/15/egy_kis_lepes_a_szemelyes_adat_fogalmanak_relativ_ertelmezese_fele (letöltés: 2023. 12. 10.)

¹⁵⁵ EUB-ítélet C-319/22. sz. ügy

¹⁵⁶ Nadezsda PURTOVA: *The law of everything. Broad concept of personal data and future of EU data protection law.* Law, Innovation and Technology 2018/10. 78–79. <https://doi.org/10.1080/17579961.2018.1452176> (letöltés: 2023. 12. 20.)

utal a GDPR módosítását (is) célzó digitális omnibusz csomag javaslata: „egy természetes személyre vonatkozó információ nem feltétlenül személyes adat minden más személy vagy szervezet számára pusztán azért, mert egy másik szervezet azonosítani tudja az adott természetes személyt.”¹⁵⁷ A javaslat szerint tehát a személyes adat mobil fogalommá válik, ugyanaz az adat egyik vállalat számára személyes adat, a másik számára nem az. Visszatérve a jogesethez, míg a hatályos GDPR alapján a VIN személyes adat lehet, addig a csomag javaslata alapján attól függően válik személyes adattá, hogy adott gazdasági szereplő képes-e azonosítani. Azzal egyetértek, hogy a csomag intézkedni kíván a személyes adat túl tág értelmezése ellen, a szubjektív megközelítés azonban kérdésessé teszi a szándékot.

A személyes adatokon belül a GDPR elkülöníti a különleges, más szóval érzékeny adatok kategóriáit. Az elkülönítés oka az, hogy a természetes személy alapvető jogaira és szabadságaira nézve – mivel az egyének életének „intimebb szféráihoz kapcsolódnak”¹⁵⁸ – nagyobb kockázatot hordoznak, ezért ezek kezelése fokozott, magasabb szintű védelmet kíván.¹⁵⁹ A személyes adatok különleges kategóriáit a faji, etnikai származásra; a politikai véleményre; a vallási vagy világnézeti meggyőződésre; valamint a szakszervezeti tagságra utaló személyes adatok jelentik.¹⁶⁰ A személyes adatok mindezen különleges kategóriái az emberrel mint társadalmi lénnel kapcsolatos adatokat tartalmazzak, melyek az egyén sajátos helyzetét vagy nézőpontját hordozzák. Fokozott védelmüket az indokolja, hogy a történelem számos példát szolgáltatott arra, hogy az e kategóriákba sorolt adatok, vélemények és véleménykülönbségek az ember magánszférájába való legsúlyosabb beavatkozáshoz vezettek (faji-etnikai összetűzések, vallásháborúk stb.).

A személyes adatok különleges kategóriáinak másik csoportja az emberrel mint biológiai lénnel kapcsolatos adatokat tartalmaz, ide tartoznak a genetikai adatok (biológiai minta elemzéséből származó, a természetes személy örökölt vagy szerzett genetikai jellemzőire vonatkozó személyes adatok, amelyek fiziológiai vagy egészségi állapotra vonatkozó egyedi információt hordoznak)¹⁶¹ és a biometrikus adatok. Utóbbi azt jelenti, hogy a természetes személyt nem külső kód alapján különböztetik meg, hanem valamilyen egyénspecifikus biológiai jegy alapján, amely lehet az ujjlenyomat, az íriszmintázat, az arckép, a DNS stb.

¹⁵⁷ Digitális omnibusz csomag javaslata 3. cikk 1. a) pont

¹⁵⁸ PÉTERFALVI Attila – RÉVÉSZ Balázs – BUZÁS Péter (szerk.): *Magyarútat a GDPR-ról*. Bp., Wolters Kluwer Hungary, 2021. 74.

¹⁵⁹ GDPR (51) preambulumbekzdés. A Charta védelme is kiterjed ezekre: „Tilos minden megkülönböztetés, így különösen a nem, faj, szín, etnikai vagy társadalmi származás, genetikai tulajdonság, nyelv, vallás vagy meggyőződés, politikai vagy más vélemény, nemzeti kisebbséghez tartozás, vagyoni helyzet, születés, fogyatékoság, kor vagy szexuális irányultság alapján történő megkülönböztetés.” (21. cikk)

¹⁶⁰ GDPR 9. cikk

¹⁶¹ GDPR 4. cikk 13. pont

Az arcfelismerő technológia, amennyire népszerű, legalább annyi kockázatot hordoz az érintett magánéletének és személyes adatai védelmére vonatkozóan. „A kockázatok mérsékléséhez vezető első lépés tehát annak tudatosítása lenne, hogy az arckép- [...] azonosítás egyáltalán nem megbízható módszer.”¹⁶² Általa a biometrikus adat, a profil „közvetlenül, véglegesen, megváltoztathatatlanul és letagadhatatlanul kapcsolódik”¹⁶³ az egyénhez, ezért olyan azonosító kódnak tekinthető, amely megfelelő háttéradatbázissal univerzális kódként funkcionálna, és nemcsak egységes hozzáférést biztosítana minden személyes adatunkhoz, de számtalan olyan adat is kinyerhető lenne általa, amelyek a hivatali ügyintézésen kívül is „számon tarthatják” egész létünket, és „mindenkinek azzal kellene számolnia, hogy titokban folyamatosan, automatikusan megfigyelhetik, ha kilép a lakásból.”¹⁶⁴

Az emberrel mint biológiai lénnel kapcsolatos adatok közé tartoznak a szexuális életére vagy szexuális irányultságára vonatkozó személyes adatok, valamint az egészségügyi adatok. Utóbbiak „egy természetes személy testi vagy pszichikai egészségi állapotára” vonatkoznak, „ideértve a természetes személy számára nyújtott egészségügyi szolgáltatásokra vonatkozó olyan adatot is, amely információt hordoz a természetes személy egészségi állapotáról.”¹⁶⁵ Idetartoznak az érintett betegségével, fogyatékosságával, betegségkockázatával, kórtörténetével, kezelésével vagy állapotával kapcsolatos információk; amelyeknek forrása a nyilvántartásba vételtől, a tényleges szolgáltatásnyújtáson, vizsgálatokon, teszteken, eszközökön át az orvosig, egészségügyi alkalmazottig terjedhet.¹⁶⁶

A személyes adatok különleges kategóriáinak kezelését a GDPR főszabályként tiltja,¹⁶⁷ de számos feltételt is meghatároz, amelyek teljesülése esetén – megfelelő garanciák mellett – megengedi azt. E feltételek közé tartozik az érintett hozzájárulása, a foglalkoztatást vagy szociális védelmet szabályozó jogi előírások, alapítvány vagy nonprofit szervezet jogszerű tevékenységéhez szükségesség, közérdek, munkahelyi egészségügyi cél, statisztikai cél stb.,¹⁶⁸ vagyis ha az adatkezelés érdeke erősebb, és általa nagyobb előny realizálódhat. Például egy roma tanulók számára kiírt pályázatra jelentkezés során igazolni kell a származást, ezt a pályázat adatlapján is szerepeltetni kell, de ettől értékesebb az, amit a pályázat nyújthat. Ugyanakkor ebben az esetben is nagyon fontos a célhoz kötöttség és az adattakarékosság.

¹⁶² G. KARÁCSONY Gergely: „Ideje megváltoztatni” – Az arcfelismerő rendszerek alkalmazásának alapjogi kockázatai a közösségi média és a deepfake korában. In: TÖRÖK Bernát – ZÖDI Zsolt (szerk): *Az internetes platformok kora*. Bp., Ludovika Egyetemi Kiadó, 2022. 309–310.

¹⁶³ NAIH-2264-2/2014/J.

¹⁶⁴ NAIH-2264-2/2014/J.

¹⁶⁵ GDPR 4. cikk 15. pont

¹⁶⁶ GDPR (35) preambulumbekzdés

¹⁶⁷ GDPR 9. cikk (1) bekezdés

¹⁶⁸ GDPR 9. cikk (2)–(3) bekezdés

Nem mindig egyszerű eldönteni, hogy egy információ személyes adatnak minősül-e, erre láttuk példának a VIN-azonosítót. Az is előfordulhat, hogy egy fénykép szolgál a természetes személy azonosítására. Ebben az esetben adott fotó személyes adat, de ha „speciális eszközzel kezelik”¹⁶⁹ ezt a fotót, például ez alapján arcmintha készül azonosítás céljából, akkor biometrikus adatnak minősül, tehát a különleges adatok közé tartozik. Hiába technológiasemleges tehát a személyes adat definíciója, a technológia fejlődése megnehezítheti az azonosíthatóságot éppúgy, mint a kategóriába sorolást, ami azonban meghatározza azokat a szabályokat, amelyeket a kezelése során be kell tartani.

3.4.1. Álnevesítés és anonimizálás

A GDPR a személyes adatokon belül csupán a különleges adatok kategóriáját különíti el, és noha az álnevesítést, mint személyesadat-kezelési módszert, technikát¹⁷⁰ megnevezi, ez nem azt jelenti, hogy új személyesadat-kategóriát hozna létre. Ugyanakkor használja az „álnevesített személyes adatok” kifejezést, és meghatározásként hozzáteszi, hogy „amelyeket további információ felhasználásával valamely természetes személlyel kapcsolatba lehet hozni.”¹⁷¹ Ez mutat rá az álnevesítés lényegére, de míg itt a természetes személlyel való azonosíthatóságra helyezi a hangsúlyt, avagy az álnevesített adat visszaállíthatóságára, addig a GDPR a fogalommeghatározásában ellenkező nézőpontból fogalmaz: „további információk felhasználása nélkül többé már nem állapítható meg, hogy a személyes adat mely konkrét természetes személyre vonatkozik.”¹⁷² Ennek teljesülését két feltételhez köti: a további információkat külön kell tárolni, valamint technikai és szervezési intézkedéseket¹⁷³ szükséges végrehajtani.¹⁷⁴ A további információk olyan kódokra, kulcsokra utalnak, amelyek által a névtelen azonosíthatóvá válik, mint ahogy a titkosítás is megfejthető a hozzá tartozó kóddal. Az álnevesítéssel létrejött adat a fentiekből következően nem veszíti el személyes adat jellegét, hiszen kulcsokkal feloldható a névtelenségből, tehát továbbra is védendő, a GDPR hatálya alá

¹⁶⁹ GDPR (51) preambulumbekkezdés és 4. cikk 14. pont

¹⁷⁰ GDPR 4. cikk 5. pont

¹⁷¹ GDPR (26) preambulumbekkezdés

¹⁷² GDPR 4. cikk 5. pont

¹⁷³ Ezekre vonatkozóan ajánlásokat fogalmaz meg: Pseudonymisation techniques and best practices Recommendations on shaping technology according to data protection and privacy provisions. 2019. [Guidelines on shaping technology according to GDPR provisions.pdf](#); ill. az EDPB álnevesítési iránymutatásokat fogadott el: Guidelines 01/2025 on Pseudonymisation Adopted on 16 January 2025, melynek nyilvános konzultációja 2025. február 28-ig tartott. [edpb guidelines 202501 pseudonymisation en.pdf](#) (letöltés: 2025. 02. 02.)

¹⁷⁴ GDPR 4. cikk 5. pont

tartozó adat, de csökkenti a kockázatokat az érintettek szempontjából, valamint segítséget nyújt az adatkezelők számára az adatvédelmi kötelezettségeiknek való megfelelésben.¹⁷⁵

Az álnevesítés görög eredetű neve, a pseudo-anonimizáció azt sugallja, hogy a titkosítás 'ál, hamis,' a névtelenség csak 'látszólagos'. Ezzel szemben az anonimizálás elnevezés jóval biztosabb névtelenséget ígér. Az anonimizálás a személyes adatokra vonatkozó olyan eljárás, amelynek eredményeként az adatok már nem kapcsolhatók össze azonosított vagy azonosítható természetes személlyel, vagyis az érintett többé már nem azonosítható. Az álnevesítés és az anonimizálás közötti alapvető különbséget tehát a „helyreállíthatóság kritériuma”¹⁷⁶ hordozza. Ebből következően az anonimizált adatok nem minősülnek személyes adatoknak, így nem tartoznak a GDPR hatálya alá sem.¹⁷⁷ E tény miatt használják gyakran olyan személyes adatok esetében, amelyeket még nem akarnak törölni, de a korlátozott tárolhatóság és a célhoz kötöttség elvének megfelelés alapján azok nem kezelhetők tovább.¹⁷⁸

Az anonimizálás nem mindenható módszer, néha az is előfordul, hogy azonosíthatóvá válik az anonim adat, különösen akkor, ha az integrált adatsorok plusz „háttértudás”¹⁷⁹ képlet érvényesül, azaz az adatsor valamely eleme egyéb forrással egészül ki, például egy ismert emberre vonatkozik. Ennek jelentősége a GDPR alkalmazása előtt és után egyaránt fölmerül, ezt mutatják a következő jogesetek. 2016-ban korabeli bűnügy témájú, konkrét nevekhez köthető iratokra vonatkozóan kértek kutatási engedélyt az egyik levéltárban, és pár héttel később több weboldalon és médiafelületen hozták nyilvánosságra az 1962-es ítéletben szereplő bűnügyet és az érintett személy nevét is. A NAIH megállapította, hogy az ítélet – mint bűnügyi személyes adat¹⁸⁰ – csak az érintett írásbeli hozzájárulásával vagy törvényi felhatalmazás alapján bocsátható rendelkezésre,¹⁸¹ továbbá hogy a levéltárnak fel kellett volna ismernie, mivel a kutató a kérelapon konkrét természetes személyeket jelölt meg, hogy anonimizálás mellett is összefüggésbe hozhatók e személyek az ítélettel.¹⁸² Adott jogesetre vonatkozóan az anonimizálással kapcsolatban körvonalazódó kérdések, amelyeket a levéltáraknak mérlegelniük kell: 1. ki értelmezi, értékeli a bűncselekményre vonatkozó adatot tartalmazó iratot; 2. az említett levéltári dolgozó ugyanaz-e, aki az adott kutatási kérelmet kezeli (hogy az

¹⁷⁵ GDPR (28) preambulumbekkezdés

¹⁷⁶ PÉTERFALVI-RÉVÉSZ-BUZÁS i. m. 116.

¹⁷⁷ GDPR (26) preambulumbekkezdés

¹⁷⁸ GDPR 5. cikk (1) bekezdés b) és e) pont

¹⁷⁹ CZAPÁRI Dóra – SZÓKE Gergely László: *Az adatvédelem és az adathasznosítás egyik kulcskérdése: a személyes adatok anonimizálása*. Jura 2022/4. 25.

¹⁸⁰ Infotv. 3. § 3. pont (b) alpont és 3. § 4. pont

¹⁸¹ Infotv. 5. § (2) bekezdés a)–c) pont

¹⁸² NAIH/2016/2504/27/H. A NAIH harmadik személy részére jogalap nélküli hozzáférés biztosítása miatt a levéltár adatvédelmi bírság megfizetésére kötelezte. A levéltár bírósághoz fordult, amely hatályon kívül helyezte a határozatot. Fővárosi Közigazgatási és Munkaügyi Bíróság: 13.K.32.793/2016/15.

anonimizálás hatékonyságát meg tudja ítélni, az összefüggést észrevesse); 3. ki végzi technikailag a műveletet. Adott jogeset nem egyedi és nem egyszeri problémát tárt fel, hanem az anonimizálással kapcsolatos módszertani megfontolásokra hívja fel a figyelmet. A Covid-járvány idején az elhunytak alapbetegségét és életkorát tartalmazó adatsorokat tettek nyilvánossá a médiában, természetesen anonim nevekkkel, de pillanatok alatt nemcsak az derült ki, hogy a járvány egyik áldozata egy brit diplomata volt, hanem az is, hogy alkoholproblémákkal küzdött.¹⁸³ A két esetből levonható az a következtetés, hogy az újrazonosítás kockázata nem zárható ki teljesen, de kontextusfüggően, a dinamikus, kockázatalapú megközelítést figyelembe vevő értékeléssel csökkenthető az esélye,¹⁸⁴ ami azt jelenti, hogy tudatosan végig kell gondolni, hogy adott anonimizálási feladat milyen összefüggések előhívását igényli. Ez azt követeli, hogy az anonimizálást az adott tárgykörben jártas, a körülményeket ismerő, a következményeket előrelátóan mérlegelni képes személy végezze.¹⁸⁵

A fenti két magyar eset mellett azt is látni kell, hogy az anonimizálás rendszerszintű problémát is jelenthet a nagy adathalmazok korában. Mobiltelefonokból kinyert anonimizált adatokból a használó életkorára 70%-os pontossággal, a nemére még nagyobb pontossággal lehet következtetni; 1,1 millió emberből közel 1 milliót lehet azonosítani négy tranzakció időpontja és helye alapján.¹⁸⁶ Ezek az adatok egyértelműen azt jelzik, hogy az anonimizálás nem megbízható módszer, és mivel a technológia fejlődésével egyre kevésbé lesz az – hiszen az anonim adat egy későbbi időpontban azonosíthatóvá válhat –, megállapítható, hogy a GDPR fogalmi rendszerének billegő elemévé vált.

3.5. Az adatkezelés, az adatkezelő és az adatfeldolgozó

A GDPR szerinti adatkezelés a személyes adatokon automatizált vagy nem automatizált módon végzett bármely műveletet jelenti.¹⁸⁷ E definíció három kulcseleme közül az a meghatározó, hogy személyes adatnak minősül-e a kérdéses adat, s ha a válasz igen, akkor

¹⁸³ LOVAS Gergő: *A brit nagykövethelyettes a koronavírus egyik áldozata Magyarországon*. Index.hu, 2020. március 25. <https://bit.ly/3qqUzwo> (letöltés: 2021. 03. 03.)

¹⁸⁴ CZAPÁRI-SZŐKE i. m. 44.

¹⁸⁵ PÉTERFALVI-RÉVÉSZ–BUZÁS i. m. 116.; Az anonimizálás technikai kérdéseit mutatja be: WP216. 29. cikk alapján létrehozott adatvédelmi munkacsoport: 05/2014. számú vélemény az anonimizálási technikákról

¹⁸⁶ Több mint tízéves adatok, ismerteti: PÜNKÖSTY András: *A nagy adathalmazok felhasználásának etikai kérdései – avagy szükség van-e adatetikára?* In: TÖRÖK Bernát – ZÓDI Zsolt: *Digitalizálódó társadalom: Tanulmányok az új technológiák társadalmi-jogi hatásairól*. Bp., Ludovika Egyetemi Kiadó, 2023. 222.

¹⁸⁷ GDPR 4. cikk 2. pont

következhethet az adatkezelés.¹⁸⁸ A „bármely művelet” kitétel azt sugallja, hogy minden, a személyes adatokkal kapcsolatos művelet ide tartozik. Ehhez segítségként a definíció maga is felsorol pár gyakori műveletet – például gyűjtés, rögzítés, rendszerezés, tagolás, tárolás, közlés továbbítás, terjesztés, összekapcsolás, törlés, megsemmisítés –, de ez nem meríti ki az összes lehetőséget. Ebből az is következik, hogy nem elegendő csak a példálózóan felsorolt lehetőségekkel összevetni az adatkezelőnek a tevékenységét. Az adatkezelés definíciójának harmadik eleme az, hogy bármely művelet végezhető automatizált vagy nem automatizált módon is. Automatizált adatkezelésnek tekinthetők az automatizált eszköz útján, így számítógéppel végzett adatkezelések; a nem automatizált kezelés a kézi, papíralapú műveleteket jelenti, amelyek akkor tartoznak a GDPR hatálya alá, ha valamely nyilvántartási rendszer részét képezik, vagy amelyeket ilyen rendszer részévé kívánnak tenni.¹⁸⁹ Nyilvántartási rendszernek minősülnek a bármilyen szempontból tagolt, strukturált állományok, amelyekben a csoportosítás lehetőséget ad a keresésre is.¹⁹⁰ A szervezetek személyügyi nyilvántartásának is gyakran van manuálisan kezelt része, amelyben a munkavállaló kizárólag papíralapon hozott dokumentumait, például a önéletrajzát, erkölcsi bizonyítványát tárolják, általában dossziékba rendezve, a név alapján ábécérendben besorolva.

Az Európa Tanács 108. számú egyezménye az egyének védelméről rendelkezik a személyes adatok gépi feldolgozása során, de lehetőség volt rá, s Magyarország vállalta is, hogy az egyezményt alkalmazza a személyes adatok nem gépi eszközökkel feldolgozott állományaira is.¹⁹¹ Ennek következményeként az Infotv. a személyes adatok kezelésére vonatkozóan eszközre és módszerre tekintet nélkül rendelkezik minden adatkezelési műveletről, mégpedig olyan módon, hogy ezekre „ex lege a GDPR anyagi jogi előírásait rendeli alkalmazni.”¹⁹²

Az adatkezelő – bármely szerv, természetes vagy jogi személy – legfőbb ismérve az, hogy „a személyes adatok kezelésének céljait és eszközeit [...] meghatározza,”¹⁹³ tehát minden, az adatkezelést érintő lényeges kérdésben dönt. A definíció jogalanyát illetően legtöbbször adott szervezet minősül adatkezelőnek, nem pedig annak vezetője vagy alkalmazottja. Még akkor is így van, ha a nagyobb szervezetek „konkrét természetes személyt jelölnek ki az

¹⁸⁸ A kutatási célú kérdőívek kitöltésére vonatkozóan azonban már az adatkezelés előtt be kell szerezni az érintett hozzájárulását, valamint előrelátóan ügyelni kell arra, hogy az adatok összekapcsolása által se legyen azonosítható egyetlen érintett sem.

¹⁸⁹ GDPR (15) preambulumbekkezdés

¹⁹⁰ GDPR 4. cikk 6. pont

¹⁹¹ 108. számú egyezmény 3. cikk 2. pont c) alpont és 27. cikk 3. §

¹⁹² Infotv. 2. § (4) bekezdés; BENDIK Tamás: *A GDPR keletkezése és a magyar jogrendszerre gyakorolt hatás*. In: PÉTERFALVI Attila (szerk.): *Személyes adatok az információs jogok felügyeletének elmúlt 25 évéből*. Bp., NAIH, 2020. 108.

¹⁹³ GDPR 4. cikk 7. pont

adatkezelés szabályainak való megfelelés biztosítása érdekében,” hiszen a felelősség ebben az esetben is a szervezeté,¹⁹⁴ a GDPR által bevezetett elszámoltathatóság elve rá vonatkozik.

Az adatkezeléssel kapcsolatos döntéshozói jogkört az adatkezelő gyakorolja, ennek során – különösen az adatkezelés célját és eszközeit illetően – meghatározza annak kulcsfontosságú elemeit, amelyekkel befolyást gyakorol a személyes adatok kezelésére. Ezek közé tartozik annak eldöntése, hogy kiknek, milyen célból és milyen típusú személyes adatait kezeli, milyen jogalap alapján, mennyi ideig, kik férnek ezekhez hozzá, ideértve azt is, hogy a kérdéses adatok személyes adatnak minősülnek-e.

Ha az adatkezelést egynél több szervezet végzi, közös adatkezelőről beszélünk. Ebben az esetben az adatkezelési célok és eszközök meghatározásában közösen vesznek részt, közösen döntenek, s a felelősség kérdéseit – amely az adatkezelésben betöltött tényleges szerepüktől függően akár eltérő is lehet¹⁹⁵ – megállapodásban rögzítik, amelynek ki kell terjednie az érintettekkel való kapcsolatra és szerepre is.¹⁹⁶ A felelősség kérdésével kapcsolatban hozott ítéletet az EUB,¹⁹⁷ amelyben az előzetes döntéshozatali kérelem arra vonatkozott, hogy az IAB Europe – a digitális marketing és hirdetési ökoszisztéma európai szintű ágazati szervezete, amely keretrendszerben dolgozott ki arra vonatkozóan, hogy a honlapszolgáltatók, a reklámpatformok jogszerűen kezeljék a felhasználók személyes adatait – közös adatkezelőnek minősül-e ez utóbbiakkal. Az EUB ítélete megállapította, hogy igen, mert az IAB „saját céljaiból befolyást gyakorol az érintett személyes adatok kezelésére, és ennél fogva tagjaival együtt meghatározza az ilyen adatkezelés céljait és eszközeit;” s ezt nem befolyásolja az a körülmény, hogy az IAB maga közvetlenül nem fér hozzá a személyes adatokhoz.¹⁹⁸

Az adatkezelő döntési kompetenciája az a pont, amely elkülöníti tőle az adatfeldolgozót. Az adatfeldolgozó két lényeges ismérve az, hogy az adatkezelőtől elkülönült szervezet (jogi személy stb.) legyen,¹⁹⁹ és az adatkezelő nevében kezelje a személyes adatokat.²⁰⁰ Ez azt jelenti, hogy a személyes adatok kezelésére vonatkozóan nincs lényeges, érdemi ráhatása. Gyakori példája ennek az, hogy ha a munkáltató kiszervezi a bérszámfejtés feladatait, akkor adatkezelőként egyértelműen meg kell határoznia, hogy „kinek, milyen összeget, mely

¹⁹⁴ EDPB: 07/2020. sz. iránymutatás az adatkezelő és az adatfeldolgozó GDPR szerinti fogalmáról 2.0 változat. 18. pont

¹⁹⁵ PÓK László: *Adalékok a közös adatkezelés megállapításához*. Blogbejegyzés, 2024. március 08. https://gdpr.blog.hu/2024/03/08/adalekok_a_kozos_adatkezes_megallapitasahoz (letöltés: 2024. 08. 21.)

¹⁹⁶ GDPR 26. cikk

¹⁹⁷ ECLI:EU:C:2024:214. A Bíróság ítélete (negyedik tanács) a C-604/22. sz. ügyben (IAB Europe és Gegevensbeschermingsautoriteit), 2024. március 7. (a továbbiakban a lábjegyzetekben: EUB-ítélet C-604/22. sz. ügy)

¹⁹⁸ EUB-ítélet C-604/22. sz. ügy 78. pont 2) alpont

¹⁹⁹ EDPB: 07/2020. 4.

²⁰⁰ GDPR 4. cikk 8. pont

időpontig, mely bankon keresztül kell fizetni, mennyi ideig kell tárolni az adatokat, milyen adatokat kell közölni az adóhatósággal stb.” Az adatfeldolgozó dönthet azonban arról, hogy a bérszámfejtési feladatot milyen technikai eszközökkel, például milyen szoftverrel oldja meg.²⁰¹

A GDPR tehát egyértelműen megkülönbözteti az adatkezelőt és az adatfeldolgozót, az adatvédelmi irányelv azonban csak az adatfeldolgozás fogalmát definiálta, az adatkezelés fogalmat egyáltalán nem használta, az implementáló Infotv. – az alább ismertetett jogvita idején – mind a két fogalmat használta és értelmezte is.²⁰² „A fogalmi zavart az okozta, hogy az irányelv [...] a kettőt gyakorlatilag összemosta. Ez azért is zavaró, mert a magyar terminológia szerinti adatfeldolgozás szűkebb jelentéstartalommal bír, mint az irányelv szerinti adatfeldolgozás.”²⁰³ Ezzel kapcsolatos kérdést terjesztett a Kúria előzetes döntéshozatal iránti kérelmében az EUB elé a NAIH és a Weltimmo, Szlovákiában letelepedett adatkezelő közötti jogvitával kapcsolatban: az adatvédelmi irányelv adatfeldolgozás fogalma azonosítható-e az adatkezelés fogalmával.²⁰⁴ Az EUB-ítélet megállapította, hogy az adatvédelmi irányelv adatfeldolgozás fogalmát azonosan kell érteni, mint az adatkezelés szót.²⁰⁵

Az adatkezelők – bár a fogalommeghatározás egyértelműen kijelöli feladataikat – nincsenek könnyű helyzetben egy-egy új technológia alkalmazási igénye esetében annak eldöntésében, hogy az a GDPR adatkezelési elveinek és követelményeinek megfelel-e. Idetartozik az arcfelismerő technológia, amelynek térnyerése odáig vezetett, hogy a repülőtereken is gyakran használják az utasok azonosítására. A francia adatvédelmi hatóság kérelmére az EDPB azt vizsgálta, hogy a repülőtéri utasforgalom egyszerűsítése érdekében végzett arcfelismerés alkalmazása során az adatkezelés összeegyeztethető-e a GDPR korlátozott tárolhatóság, integritás és bizalmas jelleg, beépített és alapértelmezett adatvédelem, valamint az adatkezelés biztonsága követelményeivel. Az értékelés szerint csak abban az esetben egyeztethető össze, ha a regisztrált biometrikus sablon vagy az utas mobiltelefonján

²⁰¹ EDPB: 07/2020. 40. pont

²⁰² Infotv. 3. § 10. pont: „adatkezelés: az alkalmazott eljárástól függetlenül az adatokon végzett bármely művelet vagy a műveletek összessége, így különösen gyűjtése, felvétele, rögzítése, rendszerezése, tárolása, megváltoztatása, felhasználása, lekérdezése, továbbítása, nyilvánosságra hozatala, összehangolása vagy összekapcsolása, zárolása, törlése és megsemmisítése, valamint az adatok további felhasználásának megakadályozása, fénykép-, hang- vagy képfelvétel készítése, valamint a személy azonosítására alkalmas fizikai jellemzők (pl. ujj- vagy tenyérnyomat, DNS-minta, íriszkép) rögzítése,” és Infotv. 3. § 17. pont: „adatfeldolgozás: az adatkezelési műveletekhez kapcsolódó technikai feladatok elvégzése, függetlenül a műveletek végrehajtásához alkalmazott módszertől és eszköztől, valamint az alkalmazás helyétől, feltéve hogy a technikai feladatot az adatokon végzik.”

²⁰³ BOJNÁR Katinka: *Egy jelentős EUB-döntés margóján*. In: SZABÓ Endre Győző (szerk.): *Az Infotörvénytől a GDPR-ig*. Bp., Ludovika Egyetemi Kiadó, 2021. 96.

²⁰⁴ ECLI:EU:C:2015:639. A Bíróság ítélete (harmadik tanács) a C-230/14. sz. ügyben (Weltimmo és NAIH), 2015. október 1. 14. pont (a továbbiakban a lábjegyzetekben: EUB-ítélet C-230/14.)

²⁰⁵ EUB-ítélet C-230/14. 66. pont 3) alpont

van, vagy a hozzá tartozó kód/kulcs van az utasnál. Ezek a lehetőségek is csak megfelelő biztosítékok érvényesítése mellett és az adatmegőrzési idő minimalizálásával alkalmazhatók.²⁰⁶ Erre a problémára reagál a digitális omnibusz csomag javaslata is, amely lényegében az EDPB említett állásfoglalását fogadja el: személyazonosság megerősítéséhez szükségesség esetén kezelhetők biometrikus adatok, amennyiben vagy azok, vagy „az ellenőrzéshez szükséges eszközök kizárólag az érintett ellenőrzése alatt állnak.”²⁰⁷

4. Az érintett és a fogyasztó

Jelen fejezetet a fogyasztó fogalmának áttekintésével nyitottam, és az adatvédelemmel kapcsolatos fogalmak értelmezésével zártam. A fejezet végén az érintett és a fogyasztó fogalmának érintkezési pontjait igyekszem megvilágítani: egyrészt összehasonlítom az érintetti és a fogyasztói alanyi kört; másrészt arra a kérdésre keresek választ, hogy a platformhasználatnál összefüggésben az érintett egyúttal fogyasztóvá is válik-e.

Felidézve az érintett és a fogyasztó fogalmát, egy közös vonásuk van: a jogalanyuk a természetes személy. A fogalmak körülhatárolásából és a dolgozat korábbi részeiből kidomborodnak azok a további szempontok, amelyek alapján az érintetti és a fogyasztói alanyi kör összehasonlítható, ezt mutatja a 2. táblázat.

2. táblázat: Az érintetti és a fogyasztói alanyi kör összehasonlítása

Szempont	GDPR: érintett	Fogyasztóvédelmi jog: fogyasztó
Jogszabály célja	védelem a személyes adatok kezelése tekintetében	gazdaságilag gyengébb fél védelme
Védelem jellege	alapjogi	gazdasági jogi
Jogalany	természetes személy	természetes személy
Jogviszonyhoz kötöttség	nem	igen (szerződés)
Szakmai célhoz kötöttség	nem releváns	kizáró tényező
Alanyi kör terjedelme	tág	szűkebb
Jogalanyi minőség jellege	adatkezeléshez kötött	ügyletkez köté, szerepfüggő

Forrás: saját szerkesztés a GDPR és a fogyasztóvédelmi uniós jogszabályok alapján

²⁰⁶ EDPB: 11/2024. sz. vélemény a repülőtéri utasforgalom egyszerűsítése érdekében az arcfelismerés alkalmazásáról (összeegyeztethetőség az általános adatvédelmi rendelet 5. cikke (1) bekezdésének e) és f) pontjával, valamint 25. és 32. cikkével) 1.1. verzió. 1–4.

²⁰⁷ Digitális omnibusz csomag javaslata 3. cikk 3. a) pont

Bár a GDPR és a fogyasztóvédelmi jogszabályok alanya is a természetes személy, de a vonatkozó jogszabályok célja, a jogviszonyhoz kötöttség és a gazdasági célhoz kötöttség alapján különböznek. A szempontsor további kulcseleme a jogalanyi minőség. A természetes személy a személyes adatai kezelése által válik érintetté. A fogyasztói minőség több összetevőből építkezik: nem szakmai célú ügylethez kötött és szerződéses viszonyban értelmezhető, ami feltételezi a másik felet, a vállalkozást is. Ha a természetes személy ezen összetevők által meghatározott minőségében jár el, akkor fogyasztóvá válik. A fogyasztói minőség szerepfüggő is, mivel adott személy egyik alkalommal fogyasztói, a másik alkalommal nem fogyasztói minőségben értelmezhető, gondoljunk arra, hogy telefont vásárolhat magánszemélyként, de vásárolhat vállalkozóként is a cége számára.

Minden fogyasztó lehet érintett (ha a személyes adatait kezelik), de nem minden érintett fogyasztó is egyben; metszéspontjukban pedig az a természetes személy helyezkedik el, aki nem üzleti célból szerződik, és a személyes adatait kezelik. Ők nem mások, mint a digitális szolgáltatást igénybe vevő fogyasztók. Ha például a természetes személy ún. ingyenes szolgáltatást vesz igénybe – például a Google-t használja –, akkor az általános szerződési feltételeket el kell fogadnia, tehát szerződéses jogviszony, ezáltal fogyasztói jogviszony keletkezik; valamint a GDPR-nak is jogalánya lesz, tehát egyúttal érintetté is válik. E szolgáltatás nyújtójára vonatkozik a DMA, a DSA és az elektronikus hírközlési adatvédelmi irányelv is. A DSA rendelkezései a fogyasztókkal összefüggésben értelmezendők, azonban a DMA a végfelhasználókkal, az elektronikus hírközlési adatvédelmi irányelv pedig a felhasználókkal összefüggésben, de utóbbiak közül csak a természetes személyek tekinthetők fogyasztónak, és ugyanezek lesznek a GDPR érintettjei is.

A különböző szituáció által különböző elnevezésű fogyasztókra vonatkozóan azonos szabályozási cél vonatkozik. Ezt mutatja a képviseleti keresetekről szóló irányelv, amely azoknak is kollektív érdekvédelmet biztosít, akikre a vonatkozó jogszabályok nem fogyasztóként, hanem utazóként, felhasználóként, lakossági ügyfélként, érintettként stb. hivatkoznak, amennyiben azok természetes személyek, és fogyasztónak minősülnek.²⁰⁸

Előfordul az is, hogy szerződés hiányában is a GDPR jogalanyává, érintetté válik valaki. A természetes személy létfontosságú érdeke – például baleset esetén – megkívánja, hogy a mentőorvos vagy a kórház hozzájárulás nélkül is hozzáférjen a vércsoportadataihoz. Szintén nem szerződés alapján válik a GDPR érintettjévé az a természetes személy, aki egy civil szervezet előadására regisztrál. E szervezetnek azért van szüksége a résztvevők néhány adatára,

²⁰⁸ Képviseleti keresetekről szóló irányelv (14) preambulumbekkezdés

hogy a finanszírozó számára bizonyítani tudja, hogy azt a feladatot ellátta, amire a szervezet a támogatóval szerződött. (A 2. melléklet mutat rá arra, hogy az érintett – az online szolgáltatásokkal összefüggésben – mely esetekben válik egyúttal fogyasztóvá is. Az ábra nem törekszik teljességre, de kiemel néhány releváns jogszabályt.)

5. Összegzés és következtetés

Az adatvédelmi szabályozás történeti íve a technológiai kénysztől indulva az önálló alapjogi védelemig jutott, és a jogi kötőerő folyamatos erősödésével járt együtt. Eleinte nemzeti szabályozások és nemzetközi ajánlások jelentették az adatvédelmet, majd a jogilag kötelező egyezmények és irányelvek következtek, ezt pedig a széttagoltságot megszüntető rendelet követte, amely célul tűzte ki az adatok biztonságos és szabad áramlásának biztosítását is a belső piacon. Az egyenletes fejlődési folyamat értéke – álláspontom szerint – az, hogy a jelenleg hatályos szabályozás nem törölte el a múltat, hanem ráépült arra: a 108. számú egyezmény korszerűsített változata és a GDPR párhuzamos létezése azt jelzi, hogy az adatvédelem olyan többrétegű rendszer, ahol a nemzetközi megállapodások és az uniós szabályok kiegészítik egymást. A személyes adatok kezelését illetően a GDPR mércéje érvényesül több uniós adatvédelmi szabályozóban, valamint a szektorális szabályozásban is törekvés van az összhang kialakítására. Mindezek arra engednek következtetni, hogy az adatvédelem kimunkált alapokkal és egységes szabályozási kerettel bír.

Az adatvédelem a technológiai környezet és az erre adott jogi válaszok relációjaként több, kisebb-nagyobb változáson átesett kulcsfogalmat generált, amelyek mérföldkövekként alakították a szemléletét. Vajon az adatvédelmi jog kialakult fogalmai adekvátak-e a modern kor fogyasztóinak és érintettjeinek védelméhez? E fejezet alapján azt láttuk, hogy elméletileg a fogalmak szilárd és koherens rendszert alkotnak egymással, és a gyakorlatban is mindaddig jól működtek, amíg a folyamat értelmezhető és követhető volt, korunkra azonban a gyakorlati érvényesíthetőségük – véleményem szerint – erősen megkérdőjelezhető. Ennek több kritikus pontja biztosan van.

Az egyik kritikus pont az, hogy a személyes adat technológiásemleges meghatározása – mely az 1980-as évektől gyakorlatilag változatlan tartalmú – még mindig stabil keret, de egy-egy új információról ma már nehezebb eldönteni, hogy személyes adat, vagy sem, aminek hátterében gyakran az értelmezési bizonytalanságot okozó új technológiák állnak. Ebből következően a jogalkalmazók több kihívással szembesülnek; de a kihívások az adatkezelők vonatkozásában is jelen vannak, akár a személyes adatok GDPR-nak megfelelő kezelésére gondolunk, akár az álnevesítés vagy az anonimizálás problémáira. A felfoghatatlan

mennyiségű, rendszeres és rutinszerű adathasználat korában a személyes adatok rendkívül széles skálája és az anonim adatok esetleges újraazonosíthatósága olyan kockázatot hordoz, amit a jelenlegi szabályozás nem feltétlenül tud kezelni. Előbbi vonatkozásában ez azt jelenti, hogy – mivel valamely információ természetes személyhez kapcsolása az azonosíthatóságra való képességen múlik – a fejlődő technikai tudás és lehetőségek miatt folyamatos változásban van, ezért merülhetett fel például, hogy akár a járműazonosító szám is lehet személyes adat. Az anonim információkkal kapcsolatban – bár elméletileg nem teszik lehetővé az azonosíthatóságot, ezért nem is személyes adatok – több példa is rámutat arra, hogy megfelelő háttértudás birtokában visszaazonosítható a természetes személy.

Az általános személyiségi jogokból levezetett információs önrendelkezési jog több évtizede az adatvédelmi szabályozás alapvető – az érintettek és az adatkezelők egyensúlyát célzó – gondolkodásmódja. Kritikus pontot jelent az, hogy az információs önrendelkezési jog ma már inkább teher, mint valódi jog, mert az érintettek értelmezési és mennyiségi problémával néznek szembe az adatkezelési tájékoztatók olvasása és a hozzájárulásukról való döntés során, és az érthetőség és a tömörség továbbra is csak elméleti követelmény. Nézetem szerint – előrejelezve a dolgozatom II. fejezetében kifejtetteket – az egyénre terhelt felelősséget csökkenteni kell, és ezzel együtt az egyszerűsített megoldásokra kell a hangsúlyt helyezni.

Mivel mindezek háttérében a technológia progresszív fejlődése áll, az említett kritikus pontok akár a szabályozás újabb generációjához is elvezethetnek. Úgy gondolom, ez az újabb generáció majdan teret kell adjon annak a célnak, hogy az érintettek élhető digitális térben folytassák tevékenységüket, és a platformoknak – hiszen a nagy adathalmazok felhasználásáról, algoritmikus kezeléséről nem mondanak le – lehetőséget arra, hogy a társadalom előrehaladásának színterei legyenek. Jelenleg az útkeresés folyamata zajlik: a kutatók egy csoportja a szigorításban (az ex ante szabályozás erősítése) látja a megoldást, ami akár az algoritmusok auditálását is megkövetelné; míg mások az egységes adatjog mellett érvelnek, „amelyben az adat mint erőforrás nyer szabályozást,” s ami akár a platformok önkéntes monitorozási tevékenységére is építhetne.²⁰⁹ Az útkeresést jelzi az is, hogy – ismerve az EU versenytámogató céljait – az alapjogok védelmének megőrzése vagy az adatok értékteremtő erejének kihasználása, mobilizációjának új dimenziói irányában történik-e majd elmozdulás, avagy milyen fogadtatásra talál a digitális omnibusz csomag javaslata.

²⁰⁹ ZÖDI Zsolt: *A platformszabályozás megold(hat)atlan dilemmái*. In: TÖRÖK Bernát – ZÖDI Zsolt: *Digitalizálódó társadalom: Tanulmányok az új technológiák társadalmi-jogi hatásairól*. Bp., Ludovika Egyetemi Kiadó, 2023. 97.

II. FEJEZET: A SZEMÉLYES ADATOK ÉRTÉKÉNEK JELENTŐSÉGE

A technológiai fejlődés és a digitalizáció következtében megváltoztak a fogyasztási szokások, így maguk a felhasználók és a fogyasztók egyre több adatot generálnak, amelyek között növekvő számban jelennek meg a szokásaikat, vágyaikat jellemző személyes adatok. Ezek az adatok hatalmas értéket képviselnek, nem véletlen, hogy a 21. század legértékesebb erőforrásává, az új olajjá²¹⁰ váltak. Ám finomítatlanul nem igazán lehet használni; ahhoz, hogy értékes termékeket állíthassanak elő belőlük, ezeket át kell alakítani, elemezni kell. Bár dolgozatom az EU-hoz kapcsolódik, a személyes adatok értékének szemléltetésére érdemes felidézni a széles körben ismert, nagy port kavart amerikai példát. Az összegyűjtött személyes adatok elemzéséből előállított értékes termék a választók befolyásolása volt az amerikai elnökválasztási kampányban. A Cambridge Analytica nevű adatelemző cég több mint 50 millió Facebook-felhasználó személyes adatait használta fel ahhoz, hogy az ún. pszichografikus profilozás módszerével mélyreható elemzést készítsen az adatalanyokról.²¹¹ E profilok alapján, az egyéni jellemzőkhöz illeszkedve, célzott politikai reklámokat juttattak el ezekhez a személyekhez, ezzel befolyásolva az amerikai elnökválasztás végkimenetelét.²¹²

A személyes adatok átadása az internet világában való részvétel feltétele. Aki a 21. század technológiai előnyeit, így az internethez kapcsolódó bármilyen eszközt, akár csak egy okostelefont is használ, valószínűleg nem tudja, hogy a személyes adatait ki és hogyan használja, ill. hogy azok mekkora értéket képviselnek. A továbbiakban azt vizsgálom, mi teszi értékessé a személyes adatokat, hogyan adják át a felhasználók ezeket a szolgáltatóknak, és milyen szerepet játszanak a marketingfolyamatokban. Ez fölveti azt a kérdést is, hogy a felhasználók tisztában vannak-e adataik értékével, kihasználják-e a szabályozás adta lehetőségeket személyes adataik védelme érdekében. Feltételezem, hogy minél kevésbé vannak tisztában azzal, hogy a személyes adataik mekkora értéket képviselnek, annál inkább kicsúsznak a vezetőülésből az adataik feletti rendelkezési jog kapcsán, ezáltal egyre inkább megadják a lehetőséget a szolgáltatók számára, hogy hatalmas mennyiségű adatot gyűjtsenek róluk, és ezek elemzésével befolyásolják őket.

²¹⁰ A felismerést Clive Humby matematikusnak tulajdonítják. ZÓDI (2017) i. m. 21.

²¹¹ HABÓK Lilla: *Cambridge Analytica: miről szól a Facebook-botrány?* <https://www.hsw.hu/hirek/58575/facebook-scl-cambridge-analytica-pszichografikus-profilozas.html> (letöltés: 2018. 11. 24.)

²¹² BENKŐ Livia: *Magánzféra kontextusban: technológia, szakpolitika és a szociális élet integritása*. Információs Társadalom 2018/2. 124.

1. A big data és az online platformok

A felhasználókról, a fogyasztókról napjainkban óriási mennyiségű adat képződik, ami már mint big data azonosítható. A big data értékének paraméterei a sebessége, változatossága, nagysága, értéke és valódisága, pontossága;²¹³ és lényeges vonása, hogy „a fogyasztókhöz nem köthető, anonim vagy anonimizált metaadatok segítségével általánosságban lehet következtetéseket levonni.”²¹⁴ A nagy adattömeg nem önmagában hordoz értéket, hanem azáltal, hogy a változatos adattípusok kezelésével és gyors, például algoritmusokkal való feldolgozásával, következtetések levonásával új termékek, szolgáltatások hozhatók létre. Amint a személyes adatok megágyaztak a big datának és az adatgazdaságnak, azzal párhuzamosan jöttek létre és erősödnek a lehetőségeket felismerő és ennek előnyeit élvező online platformok.²¹⁵

Az online platformok a digitális gazdaság motorjai, kulcsjellemzőik is közösek: az adatot mint nyersanyagot hasznosítják, a hálózati hatások és az extrém megtérülési ráta.²¹⁶ Az adat nyersanyagként használata új termékek, szolgáltatások fejlesztését teszi lehetővé. Mivel a platformok kiterjedt felhasználókörral bírnak, ezáltal nagy mennyiségű adathoz férnek hozzá, és a big data jelenség által képesek a piac mindkét oldalának szolgálatni. A közvetlen hálózati hatás értelmében a felhasználók számának növekedése miatt a platform egyre vonzóbbá válik az újabb felhasználók számára, ami – a közvetett hálózati hatás alapján – vonzóbbá teszi a platformot az üzleti szolgáltatók számára is.²¹⁷ Mindezek extrém megtérülési rátát eredményeznek, mert online környezetben gyorsan és olcsón érhető el bármely érintett szereplő.

Az online platform definíciójához a jogszabályi környezetből csak a DSA ad némi fogódzót – információt tárol, tehát tárhelyszolgáltatás; és információt nyilvánosan terjeszt,

²¹³ Andreas SAHLSTEDT: *A competition policy for the digital age – An analysis of the challenges posed by data-driven business models to EU competition law.* – Uppsala Universitet, 2019. 42–45. <http://bit.ly/37EAnM> (letöltés: 2019. 01. 14.)

²¹⁴ FÉZER Tamás: *A fogyasztók adatainak és privátszférájának védelme elektronikus környezetben.* In: SZIKORA Veronika – ÁRVA Zsuzsanna (szerk.): *A fogyasztók védelmének új irányai és kihívásai a XXI. században.* Debrecen, Debreceni Egyetem Állam- és Jogtudományi Kar, 2018. 63.

²¹⁵ Különféle elnevezéseik: digitális-technológiai vállalatok, digitális monopóliumok, digitális óriáscégek, platformóriások, digitális platformok. A világ öt legnagyobb informatikai vállalatát a GAFAM (Google, Amazon, Facebook [később Meta], Apple, Microsoft) betűszóval is szokás megnevezni, közülük az utóbbi kettő működésének csak egy részét jelentik a platformszolgáltatások.

²¹⁶ Jacques CRÉMER – Yves-Alexandre de MONTJOYE – Heike SCHWEITZER: *A Competition Policy for the Digital Era.* European Commission. 2019. 19. <https://euagenda.eu/upload/publications/untitled-257961-ea.pdf> (letöltés: 2023. 02. 06.)

²¹⁷ BELÉNYESI Pál: *A digitális piacok időszzerű versenyjogi vonatkozásai. A digitális piacokra vonatkozó joggyakorlat és a kapcsolódó joggazdasági megfontolások összehasonlítása az Egyesült Államokban és az Európai Unióban.* 2015. 10. 02. 11–12. https://www.gvh.hu/data/cms1033315/12_Belenyesi_Pal_a_digitalis_piacok.pdf (letöltés: 2023. 02. 06.)

vagyis további szolgáltatásokat is tartalmaz²¹⁸ –, a szakirodalomban azonban számos meghatározással találkozunk, ezek alapján a következő jellemzőkkel írhatók körül:²¹⁹ internetalapúak, információs és kommunikációs technológiákat (a továbbiakban: IKT), algoritmikus menedzsmentet²²⁰ használnak; és a digitális gazdaság minden jellemzőjével bírnak, ezáltal képesek biztosítani a felhasználók–árúk/szolgáltatások/tartalmak–információk kapcsolatát. A felhasználók figyelmére építik üzleti modelljüket, ezért jellemző a célzott reklámozás gyakorlata; valamint az, hogy a felhasználókhoz több csatornán férnek hozzá. Innovatívak, többoldalú és folyton változó piacokon képesek működni; más tevékenységi területek felé terjeszkedéssel gyakran ökoszisztémákká²²¹ szerveződnek. A felsorolt jellemzők következtében az online platformok a felhasználók tekintetében túlhatalomra tesznek szert, függőségeket generálhatnak gazdasági, mentális, társadalmi stb. szinten, és e szintek tekintetében formáló erővel bírnak.²²²

2. A platformok és a marketingkommunikáció

A marketingkommunikáció egy gyűjtőfogalom, magában foglal minden olyan tudatos tevékenységet, amely a termék vagy a szolgáltatás iránti keresletet igyekszik növelni. Körébe tartozik a tévéreklám éppúgy, mint a közvetlen üzletszerzési üzenetek (összefoglaló nevük: direkt marketing) és a személyre szabott hirdetések.

A közvetlen üzletszerzési célú üzenetek terméket vagy szolgáltatást ajánlanak közvetlen megkeresés útján. Jellemző csatornái közé tartozik a postai levél, a telefon vagy az sms, és az internetalapú csatornák, mint az e-mail; és általában előzetes hozzájárulás szükséges hozzájuk.

²¹⁸ DSA 3. cikk i) pont, mely számos, itt nem részletezett kivételt is tartalmaz.

²¹⁹ Forrásai: BELÉNYESI i. m. 9.; COM(2016) 288 final. A Bizottság közleménye az Európai Parlamentnek, a Tanácsnak, az Európai Gazdasági és Szociális Bizottságnak és a Régiók Bizottságának: Online platformok és a digitális egységes piac: Lehetőség és kihívás Európa számára. Brüsszel, 2016. 05. 25.; HAJNAL Zsolt – GYÓRI Ágoston: *Az online platformok és piacterek felelőssége a DSA alapján*. In: KOLTAY András. *A vadnyugat vége?: Tanulmányok az Európai Unió platformszabályozásáról*. Bp., Orac Kiadó, 2024. 519–520.; ZÓDI Zsolt: *Platformok, robotok és a jog*. Bp., Gondolat, 2018. 103.

²²⁰ ZÓDI Zsolt: *A platform mint elméleti konstrukció és mint narratív keret – A platformfogalom kialakulásának története*. 32. In: TÖRÖK Bernát – ZÓDI Zsolt (szerk.): *Az internetes platformok kora*. Bp., Ludovika Egyetemi Kiadó, 2022. 17–38.

²²¹ Az ökoszisztémák különböző szereplők dinamikus és együtt fejlődő közösségei, amelyek új értéket hoznak létre, az értékkeremtés a partnerek hálózatszerű összekapcsolódásából ered. Az ökoszisztéma a mobiltelefon példájával érzékeltethető, amely több online szolgáltatást integrálhat magába: az operációs rendszert, az alkalmazásboltot, a fizetési megoldásokat, az okosotthonhoz kapcsolódó applikációkat stb. Eamonn KELLY: *Introduction: Business ecosystems come of age*. 2015. [Introduction: Business ecosystems come of age | Deloitte Insights | Business Trends](#) (letöltés: 2024. 02. 02.); Eamonn KELLY–Kelly MARCHESE: *Supply chains and value webs*. 2015. [From supply chains to value webs | Deloitte Insights | Business Trends](#) (letöltés: 2024. 02. 02.); CRÉMER–MONTJOYE–SCHWEITZER i. m. 33.

²²² ZÓDI (2022) i. m. 76.; HAJNAL Zsolt: *The New Liability Forms of Online Platforms in the New European Digital Legal Framework from the Consumers' Perspective*. Acta Universitatis Sapientiae Legal Studies 2023/2. 20–21.

Webshopok hírlevelére például önként iratkoznak fel az emberek, mert az akciókról értesítést kapnak.

Online környezetben szinte mindenki találkozott már azzal a jelenséggel, hogy miután rákeresett valamely termékre, utazásra stb., a következő napokban folyamatosan olyan hirdetésekkel találkozik, amit a rendszer küld neki. Ennek hátterében az online platformok többségének üzleti modellje áll, amely két fontos elemre épül, arra az alaptevékenységre, ami miatt a felhasználók regisztrálnak vagy belépnek valamely webhelyre, valamint online hirdetési szolgáltatásra. Előbbi által gyűjtik a felhasználók személyes adatait, felméri a gyengeségeiket, elemzi a várható jövőbeni magatartásukat; s utóbbi által személyre szabott reklámokat jelenítenek meg számukra. E célzott kereskedelmi kommunikációs stratégia legfőbb jellemzője, hogy alkalmas a felhasználók döntésének befolyásolására, ami vonzóvá teszi a platformokat az üzleti vállalkozások, a hirdetők számára. A platformok így monetizálják a személyes adatokat, s ebből finanszírozzák a működésüket, az „ingyenes” szolgáltatásaikat, és emellett profitot is termelnek. Valószínű, hogy az ilyesfajta reklámozás hatékonyabb, mint a nem célzott hirdetések, és hogy több bevételhez juttatják a webhelyek megjelenítőit.²²³ Az adatgyűjtéstől a profilalkotáson át a konkrét üzenetek célba juttatásáig tartó teljes folyamatot – a vonatkozó EDPB-vélemény nyomán – megcélzásnak nevezik.²²⁴

Az uniós adatvédelmi szabályozás a GDPR-ban és az elektronikus hírközlési adatvédelmi irányelvben van lefektetve. A GDPR közvetlenül alkalmazandó valamennyi tagállamban, az említett irányelv rendelkezéseit a hazai jogalkotók a gazdasági reklámtevékenységről szóló törvénnyel²²⁵ implementálták. Ezenkívül 2019-ben hatályba lépett a GDPR végrehajtása érdekében szükséges törvénymódosításokról szóló törvény (a továbbiakban: adatvédelmi salátatörvény),²²⁶ amelynek a közvetlen üzletszerzéssel kapcsolatos rendelkezéseit is figyelembe kell venni az adatkezelőknek.

3. Az online platformok adatgyűjtési módszerei

A felhasználókról három módszerrel gyűjthető adat. Elsőként kell említeni az aktív rendelkezésre bocsátást, melynek során maga a felhasználó osztja meg önként az adatait.

²²³ Frederik J Zuiderveen BORGESIU – Sanne KRUIKEMEIER – Sophie C BOERMAN – Natali HELBERGER: *Tracking Walls, Take-It-Or-Leave-It Choices, the GDPR, and the ePrivacy Regulation*. EDPL 2017/3. 2. https://www.ivir.nl/publicaties/download/EDPL_2017_03.pdf (letöltés: 2018. 12. 05.)

²²⁴ EDPB: 8/2020. sz. iránymutatás a közösségi média felhasználóinak megcélzásáról. 2.0. változat. 5.

²²⁵ 2008. évi XLVIII. törvény a gazdasági reklámtevékenység alapvető feltételeiről és egyes korlátairól (a továbbiakban: Grt.)

²²⁶ 2019. évi XXXIV. törvény az Európai Unió adatvédelmi reformjának végrehajtása érdekében szükséges törvénymódosításokról

Egyszerű példaként említhetők az ingyenesen igénybe vehető közösségi platformok, mint a Facebook vagy az X (Twitter), ahol az adatalany hozza létre közösségi hálózati profilját. Szintén szándékosan bocsátja rendelkezésre személyes adatait a fogyasztó az online vásárlásoknál, legyen szó kézbesítési címéről vagy bankkártyaadatairól. Ezzel szemben a passzív rendelkezésre bocsátás esetében a felhasználónak nem áll szándékában személyes adatait átengedni, azok mégis megfigyelhetők valamely rögzítési tevékenység miatt. Idetartoznak a keresőmotorok igénybevétele során generált keresési előzmények, böngészési adatok, ill. akár az időjárás-előrejelző applikáció pontos működéséhez szükséges, helymeghatározást lehetővé tevő GPS-adatok. A felhasználók nehezen tudják ezt az adatgyűjtési módszert megérteni vagy megakadályozni. A harmadik módszer körébe tartoznak az átadott adatokból levonható következtetések: a már összegyűjtött adatokból konklúziókat megfogalmazó összetett módszer. Fontos, hogy a személyes információ levezethető látszólag „névtelen” vagy „nem személyes” adatokból is.²²⁷ Annak érdekében, hogy egy szolgáltató hozzáférjen a felhasználó személyes adataihoz, a GDPR-ban meghatározott hat adatkezelési jogalap²²⁸ közül egynek teljesülnie kell; az online platformok esetében a direkt marketing célú, személyre szabott hirdetésekre vonatkozóan általában a hozzájárulás és a jogos érdek releváns.

3.1. A személyes adatok aktív rendelkezésre bocsátása

3.1.1. A hozzájárulás

A GDPR megköveteli, hogy az érintett hozzájárulása legyen: önkéntes, konkrét, megfelelő tájékoztatáson alapuló, és egyértelműen kinyilvánított.²²⁹ A 29. cikk szerinti adatvédelmi munkacsoport iránymutatása alapján a hozzájárulás akkor önkéntes, ha az érintett valódi választási lehetőséggel bír a hozzájárulás megadása, ill. esetleges megtagadása kapcsán. Negatív következményeket nem helyezhet kilátásba az adatkezelő, és bármilyen befolyásoló elem alkalmazása érvényteleníti a hozzájárulást.

Ahhoz, hogy a hozzájárulás feltételeként a „konkrét” elem teljesüljön, az adatkezelővel szemben három követelmény támasztható. Az első követelmény a cél konkretizálása,²³⁰ hiszen a GDPR által meghatározott célhoz kötöttség elve alapján az érintettek személyes adatainak gyűjtése csak meghatározott, egyértelmű és jogszerű célból történhet, és azokat nem kezelhetik

²²⁷ OECD: *Toolkit for protecting digital consumers: A Resource for G20 Policy Makers*. 2018. 41. <https://www.consumatoriumbria.it/wp-content/uploads/2024/05/toolkit-for-protecting-digital-consumers-OEDC.pdf> (letöltés: 2022. 02. 02.)

²²⁸ GDPR 6. cikk (1) bekezdés a)–f) pont

²²⁹ GDPR 4. cikk 11. pont

²³⁰ EDPB: 5/2020. Iránymutatás az (EU) 2016/679 rendelet szerinti hozzájárulásról 1.1 verzió. 15–16.

ezekkel a célokkal össze nem egyeztethető módon,²³¹ ez egyúttal garanciát jelent az adatkezelési célok fokozatos bővülése és elmosódása ellen.²³² Tehát ha egy szolgáltató platform az eredeti céltól eltérően, más célból is kívánja kezelni az adatokat, ahhoz az érintett újabb hozzájárulását is be kell szereznie. A „konkrét” elem teljesüléséhez a cél konkrétságán kívüli egyik kritérium a hozzájárulás iránti kérelmek részletessége, vagyis az adatkezelőnek minden egyes célhoz külön hozzájárulási lehetőséget kell biztosítania; a másik kritérium a hozzájárulás megszerzéséhez kapcsolódó információk egyértelmű elkülönítése más információktól.²³³

A felhasználók, akiknek a platform a beleegyezését kéri, nem biztos, hogy értik a személyre szabott hirdetések technológiáját, a rájuk gyakorolt hatását, sőt sokszor „azzal sincsenek tisztában, hogy ilyenfajta reklámozás célpontjába kerültek.”²³⁴ Ahhoz, hogy megfelelő döntést tudjanak hozni az előzetes hozzájárulás megadása vagy megtagadása tekintetében, kellően tájékozottnak kell lenniük a későbbi adatkezeléssel összefüggésben. A tájékoztatás akkor megfelelő, ha kiderül számukra, hogy személyes adataikat hogyan gyűjtik és használják fel; azokba hogyan tekintenek bele; milyen módon és mértékben kezelik vagy fogják kezelni.²³⁵ Az idetartozó kulcsfogalom az érintett tájékoztatáshoz való joga és ezzel összefüggésben az átláthatóság (részletesen a III. fejezet ismerteti).

A hozzájárulás megadásához kapcsolódó negyedik kritérium az érintett akaratának egyértelmű kinyilvánítása. Ez mindig aktív cselekedetet vagy nyilatkozatot feltételez a felhasználó részéről, hiszen e nélkül érvénytelen a hozzájárulása. Az előre kipipált jelölőnégyzetek (checkboxok) nem fogadhatók el, ill. sem az érintett hallgatása, sem a szolgáltatás egyszerű folytatása nem tekinthető aktív lépésnek.²³⁶ A hozzájárulást nem pótolja a szerződésbe való beleegyezés és az általános szerződési feltételek elfogadása sem.²³⁷

Nem elegendő, hogy az adatkezelő a felsorolt négy kritérium betartását követően megkapja az érintett hozzájárulását, képesnek kell lennie utólag igazolni is azt.²³⁸ A bizonyításhoz szükséges módszereket maguknak kell kidolgozniuk, de tekintettel kell lenniük

²³¹ GDPR 5. cikk b) pont

²³² EDPB: 5/2020. 16.

²³³ EDPB: 5/2020. 16–17.

²³⁴ WP171. A 29. cikk alapján létrehozott adatvédelmi munkacsoport: 2/2010. számú vélemény a viselkedésalapú online reklámról. (A vélemény az adatvédelmi irányelvvel összefüggésben készült, de a viselkedésalapú reklámra vonatkozó követelményei relevánsak a GDPR-ral összefüggésben is.) 20.

²³⁵ GDPR (39) preambulumbekkezdés

²³⁶ EDPB: 5/2020. 21.

²³⁷ GDPR (32) preambulumbekkezdés; WP259. A 29. cikk szerinti adatvédelmi munkacsoport: A 29. cikk szerinti munkacsoport iránymutatása az (EU) 2016/679 rendelet szerinti hozzájárulásról. Utolsó felülvizsgált és elfogadott változat időpontja: 2018. április 10. 21.

²³⁸ GDPR (42) preambulumbekkezdés

az adattakarékosság elvére,²³⁹ a szükségesnél több információt nem gyűjthetnek annak érdekében, hogy képesek legyenek igazolni az érintett korábbi hozzájárulását.

A fentebb leírtakat figyelembe véve, az adatkezelő legitim módon jár el az adatok direkt marketing célra történő megszerzése esetén, amennyiben tájékoztatási kötelezettségének teljesítését követően megkapja az érintett megfelelő hozzájárulását adatai kezeléséhez, amelyet bizonyítani is tud. Azonban arról sem feledkezhet meg az adatkezelő, hogy az érintett jogosult arra, hogy a már megadott hozzájárulását visszavonja. A hozzájárulás bármikor visszavonható; de nem érinti a visszavonás előtti adatkezelés jogszerűségét; az érintettet tájékoztatni kell erről a jogáról; és ugyanolyan egyszerű módon kell lehetővé tenni, mint annak megadását.²⁴⁰ Ha a hozzájárulást egyetlen egérkattintással meg lehetett adni, akkor ezt a visszavonás tekintetében is biztosítani kell. Előfordulhat, hogy az érintett visszavonja a hozzájárulását, azonban az adatkezelő egy másik jogalapra történő hivatkozással tovább kezeli az adatait. Ez a gyakorlat jogilag aggályos, hiszen a szolgáltató nem tesz eleget a tájékoztatási kötelezettségének.²⁴¹

3.1.2. Tud-e az érintett tájékozott döntést hozni a személyes adatai kezelésével kapcsolatban?

A Kerber–Specht-Riemenschneider szerzőpáros által összegyűjtött szempontok alapján vizsgálom meg, hogy az érintetteknek milyen kérdésekkel kell szembenézniük a személyes adataik kezelésére vonatkozó döntések meghozatalakor az online platformok használatával kapcsolatban. Ezek a következők: az adatkezelési tájékoztató tartalma, minősége, átláthatósága; az internetes nyomon követés többféle módja; az adatkezelési tájékoztatók terjedelme; valamint a személyes adatok értéke.²⁴²

A fogyasztó és a vállalkozás közötti egyensúlyhiányból fakadó információs aszimmetria az offline és az online piacokra is jellemző, többek között ezek ellen biztosítanak védelmet a fogyasztóvédelmi rendelkezések. (Ezeket részletezi a VI. fejezet.) Az információs aszimmetria fogalma a 20. század második felében jelent meg,²⁴³ és arra utal, hogy a fogyasztó és a számára árut vagy szolgáltatást kínáló vállalkozás kapcsolata nem egyenrangú viszony. Az utóbbi

²³⁹ GDPR 5. cikk c) pont

²⁴⁰ GDPR 7. cikk (3) bekezdés

²⁴¹ EDPB: 5/2020. 29.

²⁴² Wolfgang KERBER – Louisa SPECHT-RIEMENSCHNEIDER: *Synergies between data protection law and competition law*. 2021. szeptember 30. 31. https://www.vzbv.de/sites/default/files/2021-11/21-11-10_Kerber_Specht-Riemenschneider_Study_Synergies_Between_Data%20protection_and_Competition_Law.pdf (letöltés: 2023. 02. 01.)

²⁴³ TÖRÖK Éva: *A fogyasztói szerződésekkel kapcsolatos jogalkalmazás – különös tekintettel az egyértelmű megfogalmazás követelményére*. In: SZIKORA Veronika – ÁRVA Zsuzsanna (szerk.): *A fogyasztók védelmének új irányai és kihívásai a XXI. században*. Debrecen, Debreceni Egyetem Állam- és Jogtudományi Kar (2018). 69.

mindig több információval rendelkezik az áruról, szolgáltatásról, minőségről, árakról stb., mint a fogyasztó, ami egyensúlyhiányhoz, információs aszimmetriához vezet. Mivel a GDPR a személyes adatok és a magánélet védelme tekintetében speciális fogyasztóvédelmi szabályzatnak tekinthető,²⁴⁴ fontos kérdés az, hogy a GDPR képes-e az információs aszimmetriát ellensúlyozni, és ezzel kapcsolatban az átláthatóság segíti-e a felhasználókat abban, hogy tájékozott döntést hozzanak a személyes adataik kezelésével kapcsolatban.

A vállalatok személyesadat-kezelése a GDPR alapján csak abban az esetben jogszerű, ha megfelelő jogalap áll rendelkezésükre.²⁴⁵ A jogalapok közül az érintett hozzájárulása az, amelyről magának az érintettnek kell döntenie: vagy adja a hozzájárulását, vagy nem. Döntését az adatkezelési tájékoztatóban foglaltak alapján hozhatja meg, amely arra szolgál, hogy az érintett megértse, hogy kik, mire és hogyan használják fel a beleegyezése által rendelkezésre bocsátott személyes adatokat, s hogy ezáltal fel tudja mérni a magánéletére gyakorolt hatást. Éppen azokat a folyamatokat kell végigjárnia, amelyeket azok a fogyasztók tesznek meg a jól tájékozott döntés érdekében (legalábbis elméletben), akik valamilyen terméket vásárolnak: kapcsolatba lépnek adott piaccal; összegyűjtik a fontos információkat a termékről, értékelik ezeket; majd döntenek. Ugyanígy a tájékozott beleegyezéshez az adatkezelési tájékoztatót minden regisztráció során el kell olvasni, azt értelmezni kell, majd mérlegelni az előnyöket és a hátrányokat, s végül döntenie. Ha az érintett úgy dönt, hogy hozzájárul a személyes adatai kezeléséhez, akkor a hozzájárulási nyilatkozatot aláírja, vagy kipipálja a checkboxot. Ha a tájékoztatás a GDPR elvárásainak megfelelő, akkor a hagyományos, nem adatgyűjtésre és -feldolgozásra szakosodott vállalkozások esetében az érintett valószínűleg képes lesz tájékozott döntést hozni személyes adatai kezelését illetően. Ha nem megfelelő, akkor nem tud tájékozott döntést hozni, ezt szemléltetik a következő ügyek is.

Erős fogyasztóvédelmi jellege miatt itt kell említeni a Google Allo chatkliens alkalmazás adatkezelésével kapcsolatos tájékoztatás vonatkozásában a GVH által – tisztességtelen kereskedelmi gyakorlat tilalmának feltételezett megsértése²⁴⁶ miatt – indított versenyfelügyeleti eljárást. A GVH nem azt ellenőrizte, hogy az adatkezelés a GDPR-nak megfelelően történt-e, hanem azt kifogásolta, hogy a Google nem adott közvetlen tájékoztatást a Google más termékeitől, valamint a Google-fióktól függetlenül is használható Allo chatklienssel összefüggésben (ismertetése, telepítése és használata során) a fogyasztók adatainak kezeléséről. Kiemelte, hogy a termék jellemzői közé tartozik az, hogy a Google kezeli

²⁴⁴ KERBER *i. m.* 4., TRSTENJAK *i. m.* 16.

²⁴⁵ GDPR 6. cikk (1) bekezdés

²⁴⁶ Fttv. 3. § (1) bekezdés

a személyes adatokat, tehát az erről való tájékoztatás szükséges a tájékozott fogyasztói döntéshez, enélkül a fogyasztó csak hiányos információkkal rendelkezhet a termék természetéről, a használat ellentételezéséről. Az ügy kötelezettségvállalással zárult.²⁴⁷

Miért különösen aggasztó – az elmondottakon túl is – az előző ügyben a személyes adatok kezeléséről való tájékoztatás elmaradása? Azért, mert a Google és az online platformok nemcsak egy adott, meghatározott céllal gyűjtik a személyes adatokat, hanem azokat elemzik, személyre szabott hirdetések céljával kezelik, feldolgozzák, amihez hozzátartozik a viselkedésalapú profilalkotás, az algoritmusok használata, az automatizált döntéshozatal. A személyes adatok ilyen mérvű kezelése a piaci verseny szempontjából erőfölénnyel való visszaéléshez vezethet, és belépési korlátot képezhet más vállalkozások számára; a fogyasztók szempontjából pedig az információs aszimmetriák elmélyülését, feloldhatatlan rögzülését okozhatja. Hiába határozza meg a GDPR az adatkezelési tájékoztató tartalmi, formai és nyelvi követelményeit, továbbá hiába ír elő az adatkezelők számára tájékoztatási kötelezettséget az automatizált döntéshozatal tényéről, a profilalkotásról, az ezekben az esetekben alkalmazott logikáról és az ilyen adatkezelés várható következményeiről is,²⁴⁸ ha az átlagos érintett nem érti az említett adatkezelési műveleteket, nem kompetens abban. A tájékozott döntést azonban neki kell meghoznia a személyes adatai kezelésének engedélyezését illetően, s ez azt jelenti, hogy a GDPR az érintettre hárítja a felelősség nagy részét,²⁴⁹ ezért nevezik a hozzájárulást Edwards és Veale nyomán leértékelt valutának, ezzel együtt a tájékozott beleegyezést illuzórikusnak.²⁵⁰ Ezen a helyzeten nem segít az sem, hogy a DSA az online platformok számára tiltja a profilalkotáson alapuló célzott hirdetések megjelenítését a személyes adatok különleges kategóriáinak felhasználásával, valamint tiltja kiskorúak számára.²⁵¹ A technológia folyamatos fejlődése miatt egyre aszimmetrikusabbá válik a viszony a platformok és érintettek, a felhasználók között, és az utóbbiak valószínűleg egyre nehezebben tudnak majd élni jogaikkal.

Az érintettnek – döntése meghozatalakor – szembe kell néznie azzal is, hogy az internetes nyomon követésnek számos módja és technológiája van, s az így nyert adatok egy része személyes adat. Az információs aszimmetria kialakulását a cookie-k is táplálják. Ezek a legismertebb, leginkább elterjedt, nyomkövetésre alkalmas eszközök, és böngészés közben

²⁴⁷ Vj-88/2016/71.

²⁴⁸ GDPR 13. cikk

²⁴⁹ Peter J. van de WAERDT: *Information asymmetries: recognizing the limits of the GDPR on the data-driven market*. Computer Law & Security Review 2020/38. 105436. <https://doi.org/10.1016/j.clsr.2020.105436> (letöltés: 2022. 03. 03.)

²⁵⁰ WAERDT i. m. hivatkozik a következő forrásra: Lilian EDWARDS – Michael VEALE: 'Slave to the Algorithm: Why a Right to an Explanation Is Probably Not the Remedy You Are Looking For'. Duke Law & Technology Review 2017/18. 37.

²⁵¹ DSA 26. cikk (3) bekezdés és 28. cikk

naponta többször is találkozunk velük. A webhelyek nem azonos cookie-típusokat és -elnevezéseket használnak, a kapcsolódó tájékoztató azonban elvileg elmagyarázza, hogyan használja fel adott weblap az általuk gyűjtött adatokat. De előfordult olyan eset is, hogy az adatvédelmi hatóság a cookie-kkal kapcsolatos tájékoztatóban talált kivetnivalót. A [tenyek.hu](https://www.tenyek.hu) és a [tv2play.hu](https://www.tv2play.hu) esetében a tájékozott hozzájárulás akadályaként tartalmi – nem sorolták fel tételesen a cookie-kat, nem határozták meg az egyes cookie-khoz rendelt célokat, nem volt információ a profilozásról és az adattovábbításról – és formai – a szöveg hossza, tördelése – elemeket azonosítottak, amik alapján a jogszerűtlen adatkezelésnek bírság lett a vége.²⁵²

Továbbra is kérdéses azonban, hogy miután több mint negyvenmillió fajta, köztük ismeretlen²⁵³ és káros cookie létezik, például a zombi cookie-k,²⁵⁴ sőt az internetes nyomkövetést lehetővé tevő egyéb eszközök szintén vannak, ezekről tájékoztatnak-e az online platformok. Ebben az értelemben továbbra is fennáll az információs aszimmetria, és egyelőre nincs megoldás ennek leküzdésére, hiszen az érintett továbbra sem tudja, hogy mihez adja beleegyezését, ill. még azt sem, hogy beleegyezése nélkül mely adatait és mire használják.

Az adatkezelési tájékoztatók nagy terjedelme is az információs aszimmetria forrása. A gyakran több, akár tíz-húsz oldalas dokumentum elolvasása időigényes feladat: ha az internetfelhasználók minden meglátogatott webhely tájékoztatóját elolvasnák, akkor az évi egy hónapjukat töltené ki,²⁵⁵ ami teljesen irracionális elvárás. Az általában külön kezelt cookie-tájékoztatók többnyire rövidebbek, kivéve azokat a webhelyeket, amelyek harmadik feleknek is továbbítják az adatokat, ezért mindegyik vonatkozásában tartalmaznak információt.

Az információs aszimmetriát a DMA rendelkezései – bár erősen korlátozzák a kapuőröket a különböző forrásokból származó személyes adatok kombinálása és keresztfelhasználása tekintetében – nem fogják megoldani, mert az említett adatkezelési műveletekhez egyetlen jogalapot, a végfelhasználók hozzájárulását kivételként határozzák meg,²⁵⁶ és a kapcsolódó adatkezelési tájékoztató sem lesz rövidebb, és érthetőbb sem. A bizonytalan érintettek, vagy azok, akik nem tudják felmérni adataik értékét, adataik felhasználásának következményeit, továbbra is az adatkezelési tájékoztató elolvasása és/vagy

²⁵² Gdprbirsagok.hu: GDPR bírságok. [GDPR bírságok Magyarországon](https://gdprbirsagok.hu/) (letöltés: 2023. 03. 06.) és NAIH-3195-11/2022. sz. határozat

²⁵³ Cookiepedia by OneTrust. <https://cookiepedia.co.uk/> (megtekintés: 2024. 10. 22.). A cookie-k 32%-a ismeretlen.

²⁵⁴ Ove SÖRENSEN: *Zombie-cookies: Case studies and mitigation*. London, IEEE. 321–326. [doi: 10.1109/ICITST.2013.6750214](https://doi.org/10.1109/ICITST.2013.6750214) (letöltés: 2022. 10. 21.)

²⁵⁵ Alexis C. MADRIGAL: *Reading the Privacy Policies You Encounter in a Year Would Take 76 Work Days*. 2012. március 1. [Reading the Privacy Policies You Encounter in a Year Would Take 76 Work Days - The Atlantic](https://www.theatlantic.com/technology/archive/2012/03/reading-the-privacy-policies-you-encounter-in-a-year-would-take-76-work-days/30781/) (letöltés: 2020. 01. 02.); OECD: *Toolkit...* 32.

²⁵⁶ DMA 5. cikk (2) bekezdés d) pont

megértése nélkül fognak dönteni, még akkor is, ha tudják, hogy hozzájárulásuk nélkül sem ronthatják jelentősen a kapuőrök a hozzáférést az alapvető platformszolgáltatásokhoz.²⁵⁷ A DMA említett rendelkezései ígéretes megoldásnak tűnnek a tudatos, tájékozott felhasználók számára, hiszen a szolgáltatások továbbra is ingyenesek maradnak; az adataik sorsa felől sem kell aggódniuk, ha jól döntenek a hozzájárulással kapcsolatban.

Az adatkezelési tájékoztatóval kapcsolatban felsorolt problémák könnyen ahhoz vezetnek, hogy a felhasználók előbb-utóbb tájékozottság nélkül is kipipálják a hozzájárulást jelző checkboxot. Ezt a reagálást nevezik a magatartási problémának. A személyes adatok kezeléséhez való hozzájárulás tekintetében a felhasználók magatartási problémáit leginkább az időigényes tájékoztatók elolvasása jelenti, ami oda vezet, hogy a többedik tájékoztatót már nem olvassák el, inkább beleegyeznek mindenbe, s ez megszokássá állandósul. Magatartási problémákhoz vezet a szakértelem hiánya is, a türelmetlenség; valamint az, hogy nincs tétje a felhasználó, a fogyasztó számára a beleegyezésnek mindaddig, amíg nem szerez rossz tapasztalatot. Véleményem szerint azonban ez a viselkedés csak a megnevezés szintjén fedí a magatartási probléma jelentését, valójában abszolút adekvát módon viselkednek és „válaszolnak” az információs aszimmetriához tartozó problémákra.

Álláspontom szerint az igazi veszélyt az hordozza, hogy az adatkezelési tájékoztatókra adott „válaszok” már régen rögzültek, és az érintettek nem hajlandók kilépni az évek során megkövesedett „gyakorlatból,” aktiválódott a beleegyezés-fáradtság,²⁵⁸ ami azt jelenti, hogy olyan új megközelítésre van szükség, ami egyszerűsíti az adatkezelési tájékoztatók megismerését és lényegesen csökkenti az érintettek, a felhasználók terheit. Ez az új megközelítés valószínűleg a beépített megoldásokon és/vagy automatizált rendszereken fog alapulni, ahogy azt a végberendezésekben történő személyesadat-tárolás és az adathoz való hozzáférés esetében a digitális omnibusz csomag javaslata is tartalmazza.

Úgy gondolom, hogy a beleegyezés-fáradtság enyhítése érdekében addig is meg kell követelni a felhasználóbarát jelleget, legalább azt, hogy az adatkezelési tájékoztatók kerüljék a jogi szakkifejezéseket és a terjengős megfogalmazást, valamint legyenek világosak, közérthetők és rövidek. A rövidségnek azonban ellene feszül a rendelkezésre bocsátandó információk GDPR-beli terjedelmes listája, különösen az adattovábbítást is végző vállalatok esetében, amelyek a táblázatos és tagolt, kiemeléses megoldásokkal tudják a megértést segíteni. Erőteljesen támogatná az információk értelmezését a vizuális jelölések (ikonok, piktogramok) használata is, ezek különösen jól illeszkednének a digitális környezethez. Igazi hatékony

²⁵⁷ DMA (36)–(37) preambulumbekzdés és 13. cikk (6) bekezdés

²⁵⁸ KERBER–SPECHT–RIEMENSCHNEIDER *i. m.* 33.

segítséget akkor jelentett volna, ha a GDPR alkalmazásának kezdetén vagy nem sokkal ez után már rendelkezésre álltak volna, de ez mind a mai napig nem vált gyakorlattá. A vizuális jelöléseket a GDPR megengedi, sőt a Bizottságnak „felhatalmazáson alapuló jogi aktust kell elfogadnia [...] a szabványosított ikonokkal megjelenítendő információk és az ilyen ikonok meghatározására szolgáló eljárások tekintetében.”²⁵⁹ Ez azt jelenti, hogy a jogalkotó felismerte, hogy a puszta tájékoztatás nem elegendő, különösen úgy, hogy az se nem vonzó, se nem egyértelmű.²⁶⁰ Jogi aktus azonban még nem született, ennek okai közé tartozik az, hogy az ikonok további kockázatokat okozhatnak az átláthatóságra nézve,²⁶¹ használatukkal nehéz az összes GDPR-kritériumnak megfelelni, és a géppel olvashatóságuk fogalma sem teljesen tisztázott,²⁶² tehát a kutatások még nem tudják egyértelműen támogatni a vizuális jelölések szabványosíthatóságát.²⁶³ Mindezek fölvetik azt a kérdést, hogy mivel a digitális omnibusz csomag javaslata – ha így kerül a végleges szövegbe – csak felhatalmazást ad jogi aktus elfogadására a géppel olvasható jelzések és az egykattintásos megoldások tekintetében, vajon gyorsabb lesz-e a végrehajtási és technikai eszközök kidolgozása, mint a GDPR esetében.

Nem magának a beleegyezés-fáradtságnak, hanem az információs aszimmetriának a tompítására szolgálna az iskolai oktatásban meggyökeresíteni az adatvédelem szerepének fontosságát, az információk megismerését, és tanórai gyakorlását hatékonyan megvalósítani.

3.1.3. Az úgynevezett ingyenes szolgáltatások kérdésköre

A személyes adatok értéke tekintetében bonyolult kérdést vetnek fel a nagy népszerűségnek örvendő, ún. ingyenes szolgáltatások (free-to-use services), amelyek egyrészt előnyökkel járnak, hiszen pénzbeli ellentételezés nélkül használhatók, másrészt igénybevételük aggodalomra is okot adhat a felhasználók adatainak védelme tekintetében. E körbe tartozó szolgáltatások közé sorolhatók a keresőmotorok, e-mail-szolgáltatások, a közösségi platformok – a sor szinte végeleáthatatlan a 21. században –, és a felhasználók gyakran nem is tudják, hogy

²⁵⁹ GDPR 12. cikk (7) bekezdés és (166) preambulumbekkezdés

²⁶⁰ Natali HELBERGER – Frederik Zuiderveen BORGESIU – Agustin REYNA: *The perfect match? A closer look at the relationship between EU Consumer Law and Data Protection Law*. Common Market Law Review 2017/5. 9. (pdf) https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3048844 (letöltés: 2022. 10. 11.)

²⁶¹ Rafael PESSOA: *Is an Icon Worth a Thousand Words? Grounded Legal Strategies for Standardised Icons Under the GDPR*. Tilburg Law School Tilburg Institute for Law, Technology, and Society 2023. július. 34., 49–50. <https://arno.uvt.nl/show.cgi?fid=162909> (letöltés: 2025. 12. 28.)

²⁶² Sander de JONG – Dayana SPAGNUELO: *Iconified Representations of Privacy Policies: a GDPR Perspective*. 2020. 9. DOI: [10.1007/978-3-030-45691-7_75](https://doi.org/10.1007/978-3-030-45691-7_75) (letöltés: 2025. 12. 28.)

²⁶³ Max von GRAFENSTEIN et al.: *Privacy icons as a component of effective transparency and controls under the GDPR: effective data protection by design based on art. 25 GDPR*. 23. Computer Law & Security Review: Volume 52, April 2024, 105924. <https://doi.org/10.1016/j.clsr.2023.105924> (letöltés: 2025. 12. 28.)

a szolgáltatás igénybevétele során átadott adatok valójában értéket képviselnek, csupán sodródni az árral, és élvezni az ingyenesség által kínált lehetőségeket.

A mindennapi, fizikai lét mellett ma már megkülönböztetik a digitális identitást is, utalva arra, hogy az emberi létezés aposztrofálható a digitálisan elérhető személyes adatok összességéként is. Ezek tranzakciós értékkel bírnak a gazdaságban, és a gyakorlatban új pénznemmé, fizetőeszközzé váltak.²⁶⁴ Bár az európai adatvédelmi biztos hangsúlyozta, hogy a személyes adatok nem tekinthetők árunak,²⁶⁵ a DCS-irányelv legitimálta a személyes adatok átadását a szolgáltatásokért cserében. A szabályozás célja az – elismerve egyúttal a felhasználó fogyasztó minőségét is –, hogy a fogyasztók ugyanolyan jogokkal rendelkezzenek, mint a visszterhes szerződések esetében.²⁶⁶ (Bővebben kifejtésre kerül a VI. fejezetben.) Ennek kapcsán nem egyértelmű, hogyan lehet meghatározni a személyes adatok értékét.²⁶⁷ Egy Eurobarométer felmérés tíz éve kimutatta, hogy az európaiak közel kétharmada (67%) aggódott amiatt, hogy az általuk online átadott adatokkal kapcsolatban kicsúszik az irányítás a kezükből, és tízből hét embert nyugtalanított a gondolat, hogy a vállalkozásoknak mi a célja a rendelkezésükre bocsátott adatokkal.²⁶⁸ Az eltelt évek alig változtattak ezeken az arányokon: a megkérdezettek mindössze 43%-a nyilatkozott úgy, hogy teljes mértékben kézben tartja online döntéseit.²⁶⁹ Felmerül a kérdés, hogy az adatok rendelkezésre bocsátását követően megindul-e az azokkal való kereskedelem. A válasz egyértelműen igen, a vállalkozások, a szolgáltatók egyrészt az adatok felhasználásából finanszírozzák a működésüket, másrészt jelentős profitra is szert tesznek. Végül soron az adott szolgáltató a nyertese a személyes adatokkal történő tranzakciónak, amelynek keretében a fogyasztó átadja az értékes információkat annak fejében, hogy ingyenesen használja az adott szolgáltatást.

A rendelkezésre álló rengeteg ingyenes szolgáltatás kapcsán elengedhetetlen a személyes adatok csereértékének elemzése, amelynek zsinórmértéke az információs

²⁶⁴ John ROSE – Olaf REHSE – Björn RÖBER: *Related: The Value of Our Digital Identity*. <https://www.bcg.com/en-hu/publications/2012/digital-economy-consumer-insight-value-of-our-digital-identity.aspx> 21–28. (letöltés: 2018. 11. 30.)

²⁶⁵ European Data Protection Supervisor: Opinion 4/2017 on the Proposal for a Directive on certain aspects concerning contracts for the supply of digital content. 3.

²⁶⁶ COM(2018) 183 final. A Bizottság közleménye az Európai Parlamentnek, a Tanácsnak és az Európai Gazdasági és Szociális Bizottságnak: Új megállapodás a fogyasztói érdekekért. Brüsszel, 2018. 04. 11. 2. pont

²⁶⁷ Stefan LARSSON: *Algorithmic governance and the need for consumer empowerment in data-driven markets*. <https://policyreview.info/articles/analysis/algorithmic-governance-and-need-consumer-empowerment-data-driven-markets> (letöltés: 2018. 11. 25.)

²⁶⁸ EURÓPAI BIZOTTSÁG: *A Bizottság uniós adatvédelmi reformjáról született megállapodás felfrissíti a digitális egységes piacot*. Sajtóközlemény, Brüsszel, 2015. december 15. http://europa.eu/rapid/press-release_IP-15-6321_hu.htm (letöltés: 2018. 11. 28.)

²⁶⁹ BEUC: *Connected but unfairly treated. Consumer survey results on the fairness of the online environment*. 2023. szeptember. 8. https://www.beuc.eu/sites/default/files/publications/BEUC-X-2023-113_Fairness_of_the_digital_environment_survey_results.pdf (letöltés: 2024. 12. 22.)

aszimmetria.²⁷⁰ E tekintetben az előző alfejezetben kifejtettekhez annyi kiegészítés kívánczik, hogy a big data jelenség az erőviszonyokat az adatalanyok oldaláról még hatványozottabban az adatkezelők malmára hajtja. Amikor a fogyasztó igénybe kíván venni egy adott szolgáltatást, szerződően egyetért az adatai gyűjtésével, ill. kezelésével, autonómiája mégis megkérdőjelezhető, hiszen ezeket a szerződéseket az adatkezelők egyoldalúan fogalmazzák meg, így a fogyasztói oldal hatékony részvételi lehetőségének hiánya mutatkozik e tekintetben.²⁷¹ A fogyasztók nem kerülhetnek reális alkupozícióba, az adatvédelem kívánatos szintjét illetően nem válhatnak tárgyalópartnerre, mert részükről ez olyan szakértelmet és erőfeszítést igényelne, ami biztosan nem térülne meg.²⁷² Márpedig ha a fogyasztó kénytelen belépni (hiszen előfordulhat, hogy egy adott szolgáltatás kapcsán nem talál valós alternatívát) egy olyan szerződésbe, amely beleegyezésénél fogva lehetővé teszi az állandó megfigyelését, akkor az adatkezelő megszerzett egy módszert arra, hogy a hatalmát még inkább kiterjessze a fogyasztó irányában. Az adatok elemzése és tényleges felhasználása tovább növeli az adatkezelők impériumát. Tovább lépve pedig a következő helyzet állhat fenn: ha a fogyasztó beleegyezett abba, és a szerződéses feltételek lehetővé teszik, az adatkezelők ezután harmadik felek számára is átadhatják az információt. Az ilyen harmadik felek közül kiemelkedő szerepet játszanak az adatközvetítők (adatbrókerek), akik, amelyek nem közvetlenül foglalkoznak a fogyasztókkal; ezáltal az adatok gyűjtésének és felhasználásának mértéke még kevésbé átlátható a fogyasztók számára.²⁷³ E folyamat megállítására hivatott a DMA azon rendelkezése, amely a különböző forrásokból származó adatok gyűjtését és keresztfelhasználását kötelezően hozzájáruláshoz köti.²⁷⁴ Véleményem szerint ez a rendelkezés az információs aszimmetria erősödése, a beleegyezéssel kapcsolatos magatartás rögzülése, az ún. beleegyezés-fáradtság miatt nagyságrendi változást nem fog jelenteni.

²⁷⁰ SZOMMER Károly – BALOGH Zoltán – RACSKÓ Péter: *Az on-line világban hagyott virtuális lábnyomokban rejlő információk és azok veszélyei*. Vezetéstudomány 2014/7–8. 102.

²⁷¹ Michiel RHOEN: *Beyond consent: improving data protection through consumer protection law*. Internet Policy Review 2016/1. <https://doi.org/10.14763/2016.1.404> (letöltés: 2018. 02. 02.)

²⁷² SZÓKE Gergely László: *Az európai adatvédelmi jog megújítása. Tendenciák és lehetőségek az önszabályozás területén*. (PhD-értekezés), Pécs (2014) 53. <https://ajk.pte.hu/files/file/doktori-iskola/szoke-gergely-laszlo/szoke-gergely-laszlo-vedes-ertekezes.pdf.pdf> (letöltés: 2018. 12. 05.)

²⁷³ RHOEN i. m.

²⁷⁴ DMA 5. cikk (2) bekezdés

3.2. A személyes adatok passzív rendelkezésre bocsátása

3.2.1. A jogos érdek

A GDPR alapján a jogos érdek²⁷⁵ is keletkeztethet megfelelő jogalapot a közvetlen üzletszerzési célú üzenetek küldéséhez, ami azonban nem tekinthető az adatkezelés olyan mentsvárának, amelyhez az adatkezelők jobb híján bármikor menekülhetnek. Egy vállalat jogos érdeke állapítható meg, amikor „releváns és megfelelő kapcsolat áll fenn az érintett és az adatkezelő között,”²⁷⁶ tehát azon fogyasztók tekintetében, akik már az adott cég korábbi ügyfeleinek minősülnek, küldhető direkt marketing célú üzenet a vállalat saját, hasonló termékeiről, ill. szolgáltatásairól.²⁷⁷

A jogos érdek – melynek jelentése magában foglalja azt az előnyt, amelyet az adatkezelő vagy a társadalom az adatfeldolgozásból származtathat²⁷⁸ – akkor lehet releváns jogalap, ha az érintett érdekei, alapvető jogai és szabadságai nem élveznek elsőbbséget az adatkezelőéhez képest.²⁷⁹ Ennek eldöntéséhez érdekmérlegelési tesztet kell végezni. Miután a jogos érdek pontosan megnevezésre kerül, az érdekmérlegelési tesztnek több kulcsfontosságú szempontra kell kiterjednie: az adatkezelő jogos érdekének értékelésére (törvényesnek, egyértelműnek és létezőnek kell lennie); az érintettekre gyakorolt hatás értékelésére (idetartozik a kezelendő személyes adatok jellege, az adatkezelés módja, a profilalkotás, az érintett észszerű elvárása a lehetséges adatkezelést illetően, a két fél közötti kapcsolat). Ezeken túlmenően az érdekek egyensúlyának mérlegelése is szükséges, melyhez minden más körülményt, következményt figyelembe kell venni: az érintett érdekét, alapjogainak azonosítását, hírneve megsértésének kockázatát, a kockázat bekövetkezésének lehetőségét stb. Fontos szempontot jelentenek az adatkezelő által alkalmazott további biztosítékok is: anonimizálási technikák, csak összesített adatok használata, beépített adatvédelem stb.²⁸⁰

Nem feltétlen lehetőségként, hanem az érdekmérlegelési teszt eredménye alapján javasolja számításba venni a jogos érdeket a 29. cikk szerinti munkacsoport, amely az ügyfelek igényeinek és kívánságainak érdekében a személyre szabott ajánlatok értékével érvelt.²⁸¹ Ez azonban nem eredményezheti azt, hogy az adatkezelők aránytalan mértékben ellenőrizték az

²⁷⁵ GDPR 6. cikk (1) bekezdés f) pont

²⁷⁶ GDPR (47) preambulumbekkezdés

²⁷⁷ GDPR (47) preambulumbekkezdés

²⁷⁸ WP217. A 29. cikk szerinti munkacsoport: 06/2014. számú vélemény az adatkezelő 95/46/EK irányelv 7. cikke szerinti jogszerű érdekeinek fogalmáról. (E vélemény – mivel a jogalapok tekintetében nincs lényeges különbség – a GDPR vonatkozásában is alkalmazható.) 25.

²⁷⁹ GDPR 6. cikk (1) bekezdés f) pont

²⁸⁰ WP217. 55–56.

²⁸¹ WP217. 27.

ügyfelek online és offline tevékenységeit, nagy mennyiségű, különböző forrásokból adatokat gyűjtsenek, és profilokat hozzanak létre.²⁸² A későbbi, vonatkozó EUB-ítélek azonban azt mutatják, hogy az online platformok a hirdetési célú adatkezelés során éppen ezt tették, saját érdekeik felülírták az érintettek érdekeit.²⁸³ A NAIH szerint harmadik féltől származó vagy számukra továbbított adatok esetében „erősen kétséges a jogos érdek érvényes jogalapként történő hivatkozása,” hiszen a felek között semmilyen kapcsolat nincs.²⁸⁴

3.2.2. A felhasználók eszközein elhelyezett cookie-k – az elektronikus hírközlési adatvédelmi irányelv vonatkozó rendelkezései

A platformok számára az információ összegyűjtése tekintetében hatványozott jelentőséggel bírnak a cookie-k és más nyomkövető technológiák. A személyes adatokat gyűjtő cookie-k segítségével – amelyeket általában harmadik felek helyeznek el a végberendezésen – akkor is követhetők a felhasználók, amikor már elhagyták azt a honlapot, melynek betöltődésekor települt az adott cookie. Megfigyelhető, hogy milyen webhelyeket, milyen gyakran, mennyi ideig látogat, milyen témájú cikkeket olvas, a sor a végtelenségig folytatható. Ez alapján létrehozzák a profiljukat, majd annak megfelelő személyre szabott reklámokat jelenítenek meg számukra.

A cookie-k mellett az elektronikus hírközlési adatvédelmi irányelv arról is rendelkezik, hogy automatizált hívóberendezések, faxberendezések és elektronikus levelek használata közvetlen üzletszerzési célból főszabályként kizárólag hozzájárulás alapján lehetséges, ehhez azonban egy kivételt rendel: ha az adatkezelő egy termék vagy szolgáltatás értékesítése során szerzi meg a természetes személy ügyfele elektronikus elérhetőségi adatait, akkor a saját hasonló termékeit, szolgáltatásait kínálhatja számára. Fontos követelmény, hogy minden üzenetküldés alkalmával tájékoztatást kell nyújtania arról, hogy a reklámmal célzott személy kifogással élhet az üzenetküldés ellen,²⁸⁵ ebből következően tilos elrejtetni a feladó személyazonosságát, és kötelező feltüntetni az olyan érvényes címet, amelyre a további megkeresések megtiltására vonatkozó kérés elküldhető.²⁸⁶

²⁸² WP217. 27–28.

²⁸³ ECLI:EU:C:2023:537. A Bíróság ítélete (nagytanács) a C-252/21. sz. ügyben (Facebook kontra Bundeskartellamt), 2023. július 4. (a továbbiakban a lábjegyzetekben: EUB-ítélet C-252/21. sz. ügy). 105–109. pont

²⁸⁴ NAIH/2018/3567/2/V. 5.

²⁸⁵ Elektronikus hírközlési adatvédelmi irányelv 13. cikk (1)–(2) bekezdés

²⁸⁶ Elektronikus hírközlési adatvédelmi irányelv 40. cikk

3.2.3. A hazai szabályozás

A hazai szabályozást tekintve a Grt. a közvetlen üzletszerzés jogalapjaként kizárólag a címzett előzetes, egyértelmű és kifejezett hozzájárulását jelöli meg.²⁸⁷ Ez részben megegyezik a hatályos elektronikus hírközlési adatvédelmi irányelvben foglaltakkal, azonban egy, az irányelvben foglalt lehetőséget nem tartalmaz. A hazai rendelkezések között nem található meg a vállalkozások számára az a lehetőség, hogy a már meglévő ügyfelek esetén eltekinthetnek az előzetes hozzájárulás beszerzésétől, ha biztosítják a leiratkozás lehetőségét.²⁸⁸

Az ide vonatkozó hazai szabályozás vizsgálatakor érdemes kitérni az adatvédelmi salátatörvényre is. A jogszabály alapvető célkitűzését jelentette a GDPR végrehajtásához szükséges koherencia biztosítása, amelynek keretében a direkt marketinggel kapcsolatos rendelkezéseket is tartalmaz. A Grt. által meghatározott követelmény, miszerint a direkt marketing tevékenységhez a címzett előzetes, egyértelmű és kifejezett hozzájárulása szükséges, továbbra is változatlan maradt. Kivételt jelentenek ez alól a postai direkt marketing üzenetek, amikor a címzett tiltakozását lehetővé téve, engedélyezi „egyszerre legalább 500 címzett részére feladott” küldemény kézbesítését azok előzetes hozzájárulása nélkül is.²⁸⁹

3.3. Következtetésekből származó adatok – a profilalkotás intézménye

A felhasználók internethasználatának nyomon követésével, megfigyelésével a vállalkozások, a szolgáltatók létrehozzák a profiljukat,²⁹⁰ ami alapján személyre szabott, célzott reklámot tudnak eljuttatni hozzájuk. A profilalkotás több évtizede jelen van a társadalomban, a big data jelenség azonban megváltoztatta a horderejét; míg korábban az ismert, véges számú adatok, információk alapján sorolták az egyéneket egy-egy profilba, jelenleg már hatalmas adathalmaz áll a szolgáltatók rendelkezésére.²⁹¹ Nem véletlen, hogy a felhasználók többsége aggódik a személyes adataik kezelését érintő folyamatok miatt, konkrétan 57% az előzőekben bemutatott cookie-k telepítése, és 66% a profilalkotás miatt.²⁹²

²⁸⁷ Grt. 6. § (1) bekezdés

²⁸⁸ TÓTH Krisztina: *Mi lesz veled direkt marketing?* https://jogaszvilag.hu/uzlet/mi-lesz-veled-direkt-marketing/#_ftn1 (letöltés: 2019. 06. 02.)

²⁸⁹ Grt. 6. §

²⁹⁰ Megkülönböztethetők a prediktív profilok, amelyek az egyéni és a kollektív felhasználói viselkedés hosszabb időn át történő megfigyelésén alapulnak; valamint az explicit profilok, amelyeket az érintett által pl. a regisztráció során önként rendelkezésre bocsátott személyes adataiból állítanak elő. E két megközelítés összekapcsolható, és a profil kiegészíthető azokkal a halmozott adatokkal, amelyeket olyan felhasználók viselkedéséből állapítanak meg, akik hasonló viselkedési formákat tanúsítanak más kontextusban. WP171. 8.

²⁹¹ ZÓDI (2018) i. m. 85–86.

²⁹² SWD(2024) 230 final. European Commission: *Commission staff working document fitness check of EU consumer law on digital fairness*. Brüsszel, 2024. 10. 03. 21.

A profilalkotás a személyes adatok automatizált kezelésének olyan technikája, amelyet a személyes jellemzők értékelésére használnak.²⁹³ E definíció két kulcseleme bővebb kifejtésre szorul. Először is a személyes adatok kezelése automatizált eszközök útján történik, ami az adatok gépi feldolgozását jelent, és az elemzést éppúgy magában foglalja, mint az összefüggések felismerését.²⁹⁴ Ehhez matematikai, statisztikai eljárásokat, algoritmusokat vesznek igénybe. A felismert összefüggések alkalmazása alapján valósul meg a profilalkotás másik kulcsfontosságú eleme, a személyes jellemzők értékelése,²⁹⁵ ami általában a természetes személy valamely feladat végrehajtására vonatkozó képességeinek, érdeklődési körének vagy várható magatartásának megítélésére vonatkozik.²⁹⁶ A GDPR nevesíti is a kapcsolódó célokat: „munkahelyi teljesítményhez, gazdasági helyzethez, egészségi állapothoz, személyes preferenciákhoz, érdeklődéshez, megbízhatósághoz, viselkedéshez, tartózkodási helyhez vagy mozgáshoz kapcsolódó jellemzők elemzésére vagy előrejelzésére használják.”²⁹⁷ A fogyasztói társadalomhoz ezen a ponton kapcsolódik a profilozás, a személyre szabott marketinggel a vállalatok automatikusan az egyes felhasználók kikövetkeztetett jellemzőihez, elfogultságaihoz és gyengeségeihez igazíthatják a reklámokat,²⁹⁸ tehát arra használható, hogy manipulálják őket.

A profilalkotás súlyos következményekkel járhat, hiszen eredményeképpen az érintetteket különböző kategóriákba sorolják, beskatulyázzák, ill. predikciókat készítenek róluk, ezért elengedhetetlen a megfelelő garanciák biztosítása, hogy gyakorolhassák jogaikat a profilalkotással kapcsolatban. Ennek körébe tartozik, hogy az érintettet a profilalkotás tényéről és annak következményeiről tájékoztatni kell.²⁹⁹ Szintén az érintett jogosultságai közé tartozik, amennyiben közvetlen üzletszerzés érdekében történik a profilozás, a GDPR-ban nevesített tiltakozáshoz való jog.³⁰⁰ Az érintett figyelmét e jogra kifejezetten fel kell hívni, és az erre vonatkozó tájékoztatást egyértelműen és más információtól elkülönítve kell megjeleníteni.³⁰¹

Míg azonban a GDPR, bár főszabályként tiltja a személyes adatok különleges kategóriáinak kezelését, ideértve a profilalkotást is, de bizonyos kivételekkel megengedi;³⁰² addig az EU újabb jogalkotási aktusai közül a DSA erőteljesebb tiltást fogalmaz meg: az online platformot üzemeltető szolgáltatók nem jeleníthetnek meg profilalkotáson alapuló hirdetéseket

²⁹³ GDPR 4. cikk 4. pont

²⁹⁴ WP251. A 29. cikk szerinti adatvédelmi munkacsoport: Iránymutatás az automatizált döntéshozatallal és a profilalkotással kapcsolatban a 2016/679 rendelet alkalmazásához. 7.

²⁹⁵ WP251. 7.

²⁹⁶ WP251. 7.

²⁹⁷ GDPR 4. cikk 4. pont

²⁹⁸ HELBERGER–BORGESIU–REYNA *i. m.* 22. (pdf)

²⁹⁹ GDPR 13. cikk (2) bekezdés f) pont és 14. cikk (2) bekezdés g) pont

³⁰⁰ GDPR 21. cikk (2) bekezdés

³⁰¹ GDPR 21. cikk (4) bekezdés

³⁰² GDPR 9. cikk (1)–(2) bekezdés

a felhasználók érzékeny, különleges adatai felhasználásával.³⁰³ A rendelkezés háttérében az a felismerés és cél áll, hogy a felhasználók, fogyasztók ne szembesülhessenek a gyengeségeiket könnyen kihasználó célzott hirdetésekkel.

A GDPR – noha különös védelmüket elismeri – közvetlenül nem tiltja a gyermekeket célzó hirdetéseket és a profilozásukat; a DSA azonban mindkettőt tiltja. Ez a tilalom nem vonatkozik minden online közvetítő szolgáltatóra, csak az online platformot üzemeltető szolgáltatókra (értelemszerűen az óriásplatformokra és a nagyon népszerű online keresőprogramot üzemeltető szolgáltatókra is), és összekapcsolódik azzal a feltétellel, hogy „ha kellő bizonyossággal tudatában vannak annak, hogy a szolgáltatás igénybe vevője kiskorú.”³⁰⁴ Az életkorról megbizonyosodhat a platform a magatartási kódexekben foglaltak figyelembevételével, a szülő e-mail-címére küldött megerősítő üzenettel³⁰⁵ vagy a 2024-ben a euConsent által bemutatott AgeAware alkalmazással.³⁰⁶

A megcélzásnak nevezett folyamat a személyes adatok gyűjtésével indul, és a személyre szabott üzenetek célba juttatásával zárul, amikor a platformok elhelyezik az egyes felhasználók felületein az üzeneteket. Ezzel útjára indul a kínálás, és következhet a fogyasztás; miközben a platformok, a hirdetők és a teljes ökoszisztéma azon dolgozik, hogy az egyéneket újabbnál újabb célzásokkal tegye fogyasztókká.

3.3.1. A profil felhasználása más területeken

A profilalkotás legismertebb, legláthatóbb területe a célzott reklámozás, de emellett számos területen használják még, jellemzően ott, ahol kevesebb forrást kell elosztani, mint amire igény lenne, ezért a személyes adatok automatizált, gépi kezelése által kockázatfelmérés és döntéshozatal történik. Ide tartozik a pénzügyi szektor, a foglalkoztatás, a szociális szféra, az oktatás vagy az egészségügy, amelyekben a döntés – a felállított rangsor, szempontsor alapján – az egyénekre vonatkozóan joghatással jár, vagy őket jelentős mértékben érinti. (E szektorokat foglalja össze a 3. melléklet.)

Az álláskereső által beadott pályázatokat automatizált eszközökkel szűrik, s a döntés jó esetben is csupán egy értesítés. A munkavállalók szempontjából az a fajta profilalkotás

³⁰³ DSA 26. cikk (3) bekezdés

³⁰⁴ DSA 28. cikk (1)–(3) bekezdés

³⁰⁵ Europa.eu: *A személyes adatok védelme, internetes adatvédelem* (2021). https://europa.eu/youreurope/citizens/consumers/internet-telecoms/data-protection-online-privacy/index_hu.htm. (letöltés: 2021. 04. 22.)

³⁰⁶ EUCONSENT.EU: *euCONSENT announces the AgeAware App – device-based online age assurance*. Sajtóközlemény, 2024. április 12. <https://euconsent.eu/euconsent-announces-the-ageaware-app-device-based-online-age-assurance/> (letöltés: 2024. 05. 12.)

hordozza a legtöbb kockázatot, amely nem azt értékeli, amit tett, hanem azt mutatja meg, hogy a jövőben valószínűleg hogyan fog teljesíteni, s e valószínűség alapján születnek a döntések. A teljesítmény-előrejelzést használhatják akár előléptetés, akár elbocsátás előkészítésére is, de mivel jövőbeli magatartás megállapítására irányul, gyakorlatilag nem lehet védekezni ellene.

Nincs ez másként a fogyasztókkal kapcsolatban sem. A pénzügyi szektorban a profilalkotást rendszerszinten a bankok, a hitelközvetítők és a biztosítótársaságok alkalmazzák. Fel kell mérniük a kockázatokat, meg kell határozni a feltételeket, a díjakat stb. – ezeket az ügyfél személyes adatai alapján teszik. A magánszférát érintő kockázatot hordozhat a összegyűjtött adatokból levont következtetések alapján a csoportokba sorolás, ha annak célja az adott szempontból fontos és nem fontos ügyfelek azonosítása. A csoportba sorolás alapján például a bankok diszkriminálhatnak a hitelért folyamodók között,³⁰⁷ s a minősítésük alapján határozhatják meg akár a kamatlábat is. Casco-biztosítás-kötésnél az életkor, a lakóhely, a vezetési szokások, korábbi biztosítási események stb. alapján készül a profil, s ez alapján szabják egyénre a biztosítási díjat. Ha kedvező a profil, alacsonyabb a biztosítási díj is. A profilalkotás során be kell tartani az adatkezelés minden alapelvét, ezek közül az érintetti oldalon is megjelenő tájékoztatáshoz való jog értelmében a rendelkezésre bocsátandó információk közé tartozik az „automatizált döntéshozatal ténye, ideértve a profilalkotást is [...], az alkalmazott logikára és arra vonatkozóan érthető információk, hogy az ilyen adatkezelés milyen jelentőséggel, és az érintettre nézve milyen várható következményekkel bír.”³⁰⁸ A gyakorlatban azonban, különösen a kizárólag automatizált döntés esetében, az érintett nem feltétlenül tudja – ha a kedvezőtlenebb ajánlat okait érti is –, hogyan lehet javítani a profilján, különösen akkor, ha csupán objektív tényezők (életkor, lakóhely jellege) rontják azt.

Véleményem szerint mára már olyan mértékben elterjedt a profilalkotás és az automatizált döntési folyamat, hogy szinte észrevétlenül épült be és vette át az ember helyét az élet sok területén. A profilalkotás már nemcsak módszer, nemcsak technika, hanem rendszerszintű irányvonal, ami önálló életre kelt, és tőlünk függetlenül határoz a fizetésemelésünk mértékétől a biztosítási díjtételekig mindenről. Az érintett teljesen passzív, a döntéseket készen kapja, és a mögötte álló egész technológia homályos és láthatatlan. Ezt az irányvonalat kívánja a digitális omnibusz csomag javaslata még tovább fokozni azzal, hogy a GDPR hatályos rendelkezése helyett – amely főszabályként tiltja az automatizált döntéshozatalt³⁰⁹ – lehetővé teszi az algoritmusok általi döntéshozatalt, ha szerződéskötéshez

³⁰⁷ LARSSON i. m.

³⁰⁸ GDPR 13. cikk (2) bekezdés f) pont

³⁰⁹ GDPR 22. cikk (1) bekezdés

vagy -teljesítéshez szükséges, még akkor is, ha a döntés nem kizárólag automatizált módon hozható meg.³¹⁰ Az ilyen mérvű engedékeny szabályozással határozottan nem értek egyet – bár a versenyképességet bizonyos szektorokban fokozhatja –, mert a folyamat abba az irányba tart, hogy egyre nagyobb mértékben kikapcsolódik az emberi szál, ezáltal eltolódik a teljesen gépi, automatizált rendszerek felé, és az a veszély fenyeget, hogy előbb-utóbb teljesen elsöpri a hatályos GDPR legértékesebb érintetti jogát, utat nyit a diszkriminációnak, védekezés pedig nincs ellene.

4. A személyre szabott hirdetések veszélyei

A személyre szabott hirdetések azon túl, hogy tolakodóak, képesek arra is, hogy kárt okozzanak. Az ilyen hirdetések hatásának súlyát pregnánsan érzékelteti a fejezet bevezető soraiban említett Cambridge Analytica-botrány. A célzott reklámok még az adott termék vagy szolgáltatás iránt érdeklődők számára is hordoznak olyan veszélyt, hogy meggondolatlanul, elhamarkodottan döntenek az ügylet mellett, és nem fordítanak gondot arra, hogy más forrásból is utánanézzenek a keresett terméknek.³¹¹ Előfordulhat az is, hogy valós szükséglet és vásárlási szándék nélkül szeretnek bele valamely termékbe, és meg is veszik azt. Ugyanígy elven az is megtörténhet, hogy egy-egy árucikk keresését követően a platformok magasabb árat jelölnek meg a megcélzottak számára, mint ismeretlenek számára. További kapcsolódó veszélyt jelent az, hogy a platform csak azokat a termékeket, szolgáltatásokat kínálja személyre szabottan, amelyeknek a reklámozását valamely vállalat kérte, vagyis reklámköltséget fizetett.

A célzott reklámok lehetséges negatív hatásai még erőteljesebbek lehetnek, ha gyermekeket érint. Bár a GDPR alapján a gyermekek személyes adatai „különös védelmet érdemelnek,”³¹² speciális rendelkezéseket csak az életkor meghatározására, annak ellenőrzésére és a tájékoztatási kötelezettségre vonatkozóan állapít meg,³¹³ de a marketingcélú reklámozást és a profilalkotást nem tiltja. Tiltja azonban 2024. februártól a DSA, de csak a hatálya alá tartozó online platformot üzemeltető szolgáltatók számára.³¹⁴ (Részletes bemutatása a VI. fejezetben.)

5. A személyre szabott hirdetések előnyei

Néhány esetben előfordulhat, hogy előnyökkel jár a természetes személyek számára, ha róluk információkat gyűjtenek, elemeznek. Idetartozik az az eset, ha a potenciális fogyasztót

³¹⁰ Digitális omnibusz csomag javaslata 3. cikk 7. a) pont

³¹¹ EDPB: 8/2020. 8.

³¹² GDPR (38) preambulumbekzdés

³¹³ GDPR (58) preambulumbekzdés, 8. cikk és 12. cikk (1) bekezdés

³¹⁴ DSA 28. cikk (1)–(3) bekezdés

célozzák meg, aki a megfelelő időben kapja a személyre szabott ajánlatot, továbbá folyamatos kapcsolat tartható a két fél között, s ezáltal gyorsítható a vásárlási döntési folyamat.

Még erőteljesebb előnyt mutat az az eset, amikor a felhasználók adatainak gyűjtése valamely szolgáltatás fejlesztése, optimalizálása, esetleg a szolgáltatásnak az adatalany preferenciáihoz történő igazítása érdekében történik.³¹⁵ Példaként említhető a mindennapi életből a csuklón viselhető okosóra, amelynek használatából a felhasználó és az egészségügy is profitálhat. Bizonyos típusú okosórák mérik a fizikai aktivitást, a pulzusszámot, az agyi aktivitást, a vérnyomást, a kalóriaadatokat stb. Ezeket a személyes adatokat az órához tartozó szoftveralkalmazások lefordítják és összefoglalják, majd személyre szabott visszajelzést nyújtanak azért, hogy egészségesebb életmód folytatására ösztönözzenek. Végző soron segíti a felhasználókat az életminőségük javításában és az élettartamuk növelésében. Továbbá ezek az alacsony költségű, viselhető egészségügyi monitorok forradalmasítják a klinikai vizsgálatok iparát, mivel teljes személyes egészségügyi nyilvántartást hoznak létre az adott személy vonatkozásában.³¹⁶

6. Közgazdasági-pszichológiai kitekintés

A természetes személyeket jogi szabályozás védi a nem kívánt, személyre szabott reklámmal kapcsolatban, ezáltal megfogalmazódhat a kérdés, hogy akkor miért jelent problémát, hogy a profitszerzés érdekében befolyásolni próbálják őket a vállalkozások. A választ egy rövid, a viselkedési közgazdaságtanhoz kapcsolódó kitekintés szemlélteti. A viselkedési közgazdaságtan a pszichológia és a közgazdaságtan határán helyezkedik el, a fogyasztók gazdasági viselkedését, azon belül a döntéseik és tevékenységeik hátterét vizsgálja. A marketinggel kapcsolatban a vállalatok számára a kiindulópont, hogy az „értelem és érzelem” sok esetben nem különíthető el a fogyasztók döntési folyamatában, és ez az, aminek kiaknázásából haszna származhat a vállalatoknak.³¹⁷ A kívülről érkező környezeti hatások, így a célzott reklám révén a fogyasztók hajlamosabbak lesznek kevésbé megfontolt döntéseket hozni, vagyis az érzelmi szál aktiválódhat a racionális döntésekkel szemben.³¹⁸

Példát szolgáltatnak erre azok a direkt marketing célú üzenetek, amelyek a szülőkre a gyermekeikkel kapcsolatban próbálnak hatni, hiszen ezek a fogyasztót könnyen döntésre

³¹⁵ OECD: *Toolkit...* 42.

³¹⁶ Grant ARNOW: *Apple watch-ing you: Why wearable technology should be federally regulated.* <https://digitalcommons.lmu.edu/cgi/viewcontent.cgi?article=2973&context=llr> (letöltés: 2018. 11. 23.)

³¹⁷ KOLTAY Gábor – VINCZE János: *Fogyasztói döntések a viselkedési közgazdaságtan szemszögéből.* Közgazdasági Szemle 2009/6. 495.

³¹⁸ KOLTAY–VINCZE i. m. 501.

bírhadják. Akár a jó erkölcsbe ütköző gyakorlatot is megvalósíthat egy-egy olyan eset, amikor a cégek ezekkel az üzenetekkel, ill. a reklámjaikkal azt a gondolatot igyekeznek a szülők tudatában elültetni, hogy csak az adott termék megvásárlásával tehetik boldogabbá, esetleg egészségesebbé a gyermeküket. Ezenkívül ez az érzelmi befolyásolás gyorsítja a vásárlási folyamatot, amely által a fogyasztó elesik attól, hogy megismerhesse az adott termék, ill. szolgáltatás valós alternatíváit.³¹⁹ Nem meglepő tehát, hogy az ilyen üzenetek kapcsán kevésbé körültekintővé és érzelmileg motiváltabbá, elszántabbá válnak a fogyasztók, amely által könnyen döntési hibákat követhetnek el vásárlásaik során.

7. Lehetséges védelmi mechanizmusok

A kényszerű üzletszerzési célú üzenetekkel szemben rendelkezésre álló ellenlépések, védelmi mechanizmusok a következők: megfelelő jogszabályi környezet kialakítása; nemzetközi együttműködés; fogyasztói tudatosság növelése.³²⁰

Az első és legfontosabb ellenlépés a megfelelő jogszabályi környezet kialakítása. Véleményem szerint az EU jelenlegi szabályozása egyenetlenséget mutat. A GDPR egységességet és következetességet kíván a tagállamoktól, de nem mondható el ugyanez a hírközlési ágazatban az adatvédelmi szabályozásról, hiszen továbbra is az elavult irányelv és annak implementált tagállami jogszabályai határozzák meg a védelem szintjét.

A következő védelmi mechanizmust a nemzetközi együttműködés jelenti az adatvédelem területén. Uniós fogyasztók gyakran vásárolnak tengerentúli vállalkozásoktól, regisztrálnak olyan platformokon, amelyeknek székhelye Európán kívül van, ami azzal jár, hogy adataikat harmadik országba továbbítják, ezzel együtt gyakran kapnak tőlük marketingüzeneteket is. Az adattovábbítás során is elengedhetetlen a természetes személyek védelme a személyesadat-kezelés tekintetében az európai jogszabályoknak megfelelő szinten; erről már az adatvédelmi irányelv is rendelkezett,³²¹ jelenleg pedig a GDPR előírásait kell alkalmazni. Személyes adatok továbbítását az EU-n kívülre, valamint nemzetközi szervezetek

³¹⁹ HRECSKA Renáta: *Fogyasztói döntéshozatali folyamat az információs közgazdaságtan és a viselkedési gazdaságtan eredményeinek tükrében.* 2012. 16. http://www.gvh.hu/data/cms1000468/Hrechka_Ren%C3%A1ta_tanulm%C3%A1ny.pdf (letöltés: 2019. 06. 02.)

³²⁰ VIKMAN László: *Direktmarketing és spam – lehetőségek, korlátok,* https://www.jogiforum.hu/files/publikaciok/vikman_laszlo_dm-spam%5bjogi_forum%5d.pdf (letöltés: 2019. 06. 02.)

³²¹ Adatvédelmi irányelv 25–26. cikk

részére a GDPR a Bizottság megfelelőségi határozatához köti, nem megfelelő védelmi szint esetén az adattovábbítás korlátozható.³²²

Az USA-ba irányuló adattovábbítás megfelelőségét előbb a Safe Harbor, majd az adatvédelmi pajzs intézményrendszere biztosította, ezt alkalmazta többek között a Google és a Facebook is. Maximilian Schrems osztrák állampolgár – hivatkozva arra, hogy a Facebook által az USA-ba továbbított személyes adatokat megosztják az amerikai hírszerző szolgálatokkal, ami sérti a Charta rendelkezéseit, mert nem biztosít megfelelő garanciákat az uniós polgárok számára – panaszt nyújtott be az ír felügyeleti hatósághoz.³²³ Az EUB előzetes döntéshozatalra került Schrems I és Schrems II ügyekben született ítéletek előbb a Safe Harbor, majd az adatvédelmi pajzs által biztosított védelem megfelelőségéről szóló bizottsági határozatot nyilvánították érvénytelennek. Ezután az adattovábbító és -fogadó között kötött és a Bizottság által jóváhagyott Általános Szerződési Feltételek biztosították az adattovábbítás lehetőségét az USA-ba.³²⁴ 2023-ban fogadta el a Bizottság a biztonságos és megbízható adatáramlásra vonatkozó megfelelőségi határozatot, amely megállapítja, hogy az Amerikai Egyesült Államokban, a keretben részt vevő vállalatokhoz továbbított adatok tekintetében megfelelő védelmi szint biztosított az európai polgárok számára. Az adatvédelmi keret kötelező erejű biztosítékainak körébe tartozik az amerikai hírszerző szolgálatok uniós adatokhoz való hozzáféréseinek szükséges és arányos mértékre való korlátozása, valamint Adatvédelmi Felülvizsgálati Bíróság létrehozása, amelyhez uniós magánszemélyek is fordulhatnak.³²⁵

A harmadik ellenlépést az egyének tudatosságának növelése jelenti annak érdekében, hogy egyre inkább tisztában legyenek személyes adataik értékével, és ne önként, válogatás nélkül adják az adataikat, hanem tudatosan gondolják végig, hogy mely platformnak vagy szolgáltatónak mit engedélyeznek. Ezáltal kevésbé tudják kihasználni a tájékoztatatlanságukból fakadó gyengeségeiket az őket befolyásolni kívánó cégek. Véleményem szerint az adatalanyok bele sem gondolnak abba, hogy az adat milyen jelentős értéket képvisel egy vállalkozás

³²² GDPR V. fejezet és EUROPEAN COMMISSION: *Adequacy decisions*. https://commission.europa.eu/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en?prefLang=hu (letöltés: 2024. 12. 22.)

³²³ KOZMA Zoltán – ALMÁSY Márk: *Érvénytelen az EU–USA Adatvédelmi Pajzs – Az Európai Bíróság ítéletét hozott a kiemelt jelentőségű Schrems II ügyben. Érvénytelen az EU–USA Adatvédelmi Pajzs - Az Európai Bíróság ítéletét hozott a kiemelt jelentőségű Schrems II ügyben - Jogi Fórum* (letöltés: 2024. 02. 02.)

³²⁴ ECLI:EU:C:2020:559. A Bíróság ítélete (nagytanács) a C-311/18. sz. ügyben (az EU–USA adatvédelmi pajzs által biztosított védelem megfelelősége), 2020. július 16.

³²⁵ Európai Bizottság: *Adatvédelem: az Európai Bizottság az EU és az USA közötti biztonságos és megbízható adatáramlásra vonatkozó új megfelelőségi határozatot fogadott el*. Sajtóközlemény, Brüsszel, 2023. július 10. https://ec.europa.eu/commission/presscorner/api/files/document/print/hu/ip_23_3721_IP_23_3721_HU.pdf (letöltés: 2024. 12. 12.); A Bizottság (EU) 2023/1795 végrehajtási határozata (2023. július 10.) az (EU) 2016/679 európai parlamenti és tanácsi rendelet szerint a személyes adatoknak az EU–USA adatvédelmi keret által biztosított megfelelő szintű védelméről

számára, és nem hajtják végre a szükséges technikai beállításokat annak érdekében, hogy valóban rendelkezzenek személyes adataik felett. Ezáltal könnyen válnak adathalászat áldozataivá, ami a személyes adataik marketing célokra történő felhasználásához vezethet. Az egyének konkrét lépéseket is tehetnek a kéréstlen marketingüzenetek ellen, a legegyszerűbb, bárki által könnyen elvégezhető teendők: böngészési előzmények törlése, csak az oldal működéséhez elengedhetetlenül szükséges cookie-k engedélyezése, hirdetések letiltása, leiratkozás hírlevelekről.

Az is elgondolkodtató, hogy melyek azok az ágazatok, ahol a célzott reklámok és a csoportba sorolás, a beskatulyázás után is marad szabad választási lehetősége a fogyasztónak, és körültekintő, tudatos vásárlói magatartással képes ellensúlyozni a kéréstlen, targetált reklámok hatását (a kínált terméket veszi meg, avagy több helyen néz utána és veti össze a termék jellemzőit, az árakat stb.); és melyek azok a területek, ahol legfeljebb a reklámok hatása ellen tud védekezni, de a kategorizálás, a beskatulyázás ellen nem (banki szolgáltatások, biztosítások stb., tehát jellemzően a pénzügyi szolgáltatások területe). A felsorolt esetekben más ár-érték arányt képviselnek a személyes adatok is.

Az EU tervezett jogalkotási aktusa, a DFA szabályozni kívánja a személyre szabott célzott hirdetések megjelenítését is, amely újabb védelmi hálót jelenthet a fogyasztók számára azzal, hogy célja a sebezhetőségek enyhítése.³²⁶

7.1. Hozzájárulást vagy díjfizetést megkövetelő modellek

Azok számára, akik nem kívánnak folyamatosan személyre szabott hirdetésekkel találkozni, megoldásnak tűnt az adatvédelmi szakirodalomban régóta érlelődő elképzelés, hogy az érintettek magánéletének védelme érdekében az online platformok számára lehetővé kell tenni olyan üzleti modell működtetését, amely a személyes adatok hirdetési célú kezelését hozzájárulás alapján végzi, vagy díjfizetés ellenében eltekintenek attól, hogy a felhasználókat ilyen hirdetésekkel célozzák meg.³²⁷ Az EDPB véleményt bocsátott ki a hozzájárulást vagy díjfizetést megkövetelő modellekkel (consent or pay) kapcsolatban az érvényes hozzájárulásról, amelyben az érintett vállalkozások körét a nagy online platformokkal azonosítja, amelyek – mivel nagyszámú felhasználót vonzanak, és nagy léptékű adatkezelést végeznek – konkrétan a

³²⁶ Digital-fairness-act.com i. m.

³²⁷ Részletesen elemzik: KERBER–SPECHT–RIEMENSCHNEIDER i. m. 76–77.; TÓTH András: *Fogyasztóvédelmi, adatvédelmi, médiajogi és versenyjogi eszközök együttes alkalmazása az online figyelemplacok kudarcainak kiküszöbölésére*. Infokommunikáció és Jog 2021/2. 11–12.; HAJNAL Zsolt – SIMON Rita: *Key Challenges to the Implementation of the Digital Content Directive in Hungary and the Czech Republic*. In: Naděžda ŠÍŠKOVÁ (szerk.): *Legal Issues of Digitalisation, Robotisation and Cyber Security in the Light of EU Law*. Praha, Kluwer Law International, 2024. 124–125.

DSA hatálya alá tartozó online óriásplatformokat és a DMA-ben meghatározott kapuőröket jelentik.³²⁸

A vélemény szerint a legtöbb esetben a nagy online platformok nem tudnak majd eleget tenni az érvényes hozzájárulásra vonatkozó követelményeknek, ha csak az említett két, egymást kizáró választási lehetőséget biztosítják a felhasználóknak. Ennek egyik oka az, hogy a hozzájárulás érvényessége – elsősorban az önkéntesség és az egyenlőtlen erőviszony miatt – erősen kérdéses, ezért fontos a nagy online platformoknak mérlegelni, hogy olyan egyenértékű alternatívát biztosítsanak, amely nem von magával díjfizetést, és viselkedésalapú hirdetések nélkül szolgáltat. A másik oka a felszámítandó díj összegével kapcsolatos, az EDPB azt hangsúlyozza, hogy a személyes adatok nem tekinthetők kereskedelmi árunak; valamint hogy nem szabad akadályozni az érintett választási szabadságát a valódi döntés meghozatalában.³²⁹ Ez akár azon a szinten is problémás lehet, hogy minden felhasználó megengedheti-e magának, hogy békén hagyása biztosításáért pénzzel fizessen, ill. hogy a platformok milyen elven számolják a díjat: előfizetésszerűen vagy használathoz kötötten.³³⁰ A platformoknak továbbra is figyelembe kell venni az adatkezelésük során a szükségesség és arányosság, a célhoz kötöttség, az adatminimalizálás és a méltányosság elvének való megfelelést is. Az EDPB-vélemény összességében azt sugallja, hogy a díjfizetős modell alkalmazása nem reális alternatíva sem a platformok szempontjából, sem a felhasználók szempontjából, és a Bizottság hivatalos vizsgálata szerint is sérti a modellt a DMA-t.³³¹

7.2. Védekezés a szolgáltatás devalválása ellen

A jól működő internet világában, a szabad információáramlás korában a Facebookon csak az ismerősi kör bejegyzéseiből álló hírfolyamok, a Google-on a keresésnek megfelelő találatok jelentek meg, napjainkban azonban annak vagyunk tanúi, hogy a nagy platformok csökkentik az elérhető szolgáltatások körét vagy annak minőségét. Ezt a jelenséget Cory Doctorow nyomán az enshittifikáció (kevésbé vulgárisan: elvizenyősödés) szóval jelölik,³³² a hazai szakirodalomban devalvációnak nevezik.

³²⁸ EDPB: 2024/08. sz. vélemény az érvényes hozzájárulásról a nagy online platformok által alkalmazott, hozzájárulást vagy díjfizetést megkövetelő modellekkel összefüggésben. 12–13.

³²⁹ EDPB: 2024/08. 3–4.

³³⁰ HAJNAL–SIMON i. m. 123.

³³¹ EURÓPAI BIZOTTSÁG: *A Bizottság megállapítja, hogy az Apple és a Meta megsértette a digitális piacokról szóló jogszabályt.* Sajtóközlemény, Brüsszel, 2025. 04. 23.
https://ec.europa.eu/commission/presscorner/detail/hu/ip_25_1085 (letöltés: 2025. 11. 05.)

³³² Cory DOCTOROW: *As Platforms Decay, Let's Put Users First.* EFF 2023. május 9.
<https://www.eff.org/deeplinks/2023/04/platforms-decay-lets-put-users-first> (letöltés: 2025. 12. 20.)

Fölmerül a kérdés, hogy létezik-e olyan uniós jogforrás, ami kezeli azt a helyzetet, hogy a szolgáltató már monetizálta az adatot, mégis rontja a szolgáltatást. Erre vonatkozóan egyértelműen nevesített tilalom nincs. A GDPR az adatkezelés jogszerűségét szabályozza, de nem védi az érintettet a szolgáltatás butításától. Mivel az EU elismerte a személyes adatok ellenszolgáltatásként való használatát,³³³ ez azt jelenti, hogy a felhasználó, a fogyasztó nem ajándékba, hanem szerződéses jogviszony alapján kapja a szolgáltatást, ami felvetheti az ellenérték aránytalanságának kérdését. A vonatkozó DCS-irányelv a szerződésszerűség objektív követelményeit (hibás teljesítés, tájékoztatási kötelezettségek) szabályozza, és csak minimális minőségi elvárást kapcsol a teljesítéshez: a szolgáltató nem módosíthatja a digitális szolgáltatást a szerződésszerűség fenntartásához szükséges mértéket meghaladóan, ellenkező esetben szerződésszegésként értelmezhető, és lehetővé teszi a fogyasztó számára annak megszüntetését.³³⁴ A szerződés megszüntetésére vonatkozó szabályok azonban nem kielégítőek a fogyasztó adatainak a szerződés megszűnése utáni felhasználása tekintetében, ezért a DCS-irányelvet felül kell vizsgálni az adat mint ellentételezés típusú szerződésre vonatkozóan.³³⁵ Mivel a GDPR szerint a hozzájárulás önkéntességének vizsgálatakor figyelembe kell venni, hogy a szerződés teljesítésének feltételül szabták-e a szerződés teljesítéséhez nem szükséges személyes adatok kezelését,³³⁶ és a DCS-irányelv szerint az adatért nyújtott szolgáltatás nem rontható a szükséges mértéket meghaladóan; egyik jogszabály sem ad választ a devalváció problémájára. Továbbá a DCS-irányelv az egyedi jogérvényesítésre épül, a szolgáltatás devalválása azonban kollektív fogyasztóvédelmi problémát hordoz. Valódi megoldást az jelentene, ha a DCS-irányelv definiálná és beillesztené a normaszövegbe az adat mint ellenszolgáltatás típusú (személyes adatok átadásán alapuló) szerződést, amely egyértelműsítene azt, hogy az adat gazdasági értékkel bír, tehát nem ingyenes szolgáltatást nyújt a szolgáltató, ezáltal biztosítaná a szerződő felek egyensúlyát, és a minőségi követelmények rögzítésére vonatkozóan is alapot szolgáltatna. Ez alapján a DCS-irányelvben megkövetelhető és rögzíthető lenne az, hogy a szolgáltatás minősége nem lehet gyengébb, mint a pénzügyi ellenszolgáltatáson alapuló szerződések esetében.³³⁷ Mivel a személyes adatok az alapjogi

³³³ DCS-irányelv 3. cikk (1) bekezdés

³³⁴ DCS-irányelv 8. cikk (1) bekezdés és 19. cikk (1)–(2) bekezdés

³³⁵ Cemre BEDİR: *Data as Counter-Performance: Yet Another Point Where Digital Content Contracts and the GDPR Conflict*. 2018. 46–48. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3648092 (letöltés: 2025. 12. 29.)

³³⁶ GDPR 7. cikk (4) bekezdés

³³⁷ Rui Filipe Gordete ALMEIDA: *Os dados pessoais como contraprestação nos contratos de consumo — a necessidade para a execução do contrato como fundamento de licitude do tratamento Personal data as counter-performance in consumer contracts — the necessity for the performance of a contract as a basis to ensure a lawful personal data processing*. RED 2023/2. 1–48. DOI 10.24840/2182-9845_2023-0002_0002 (letöltés: 2025. 12. 30.)

védelem körébe tartoznak, ezért az adat mint ellenszolgáltatás típusú szerződés egyelőre vitatott megoldás.

A szóba jöhető harmadik jogforrás a DMA, amely szerint „a kapuőr nem ronthatja le” az „alapvető platformszolgáltatások minőségét” akkor sem, ha a végfelhasználók nem járulnak hozzá a személyre szabott reklámokhoz, a kapuőrnek ebben az esetben „kisebb mértékű személyre szabással járó, de egyenértékű alternatívát” kell kínálni, ami „nem lehet eltérő vagy rosszabb minőségű a hozzájáruló végfelhasználóknak nyújtott szolgáltatáshoz képest.”³³⁸ A Meta előbb a díjfizetős modellel, majd a reklámszünet-megoldással reagált a rendelkezésre, utóbbinak a Bizottság általi értékelése még folyamatban van, aminek ki kell terjednie arra is, hogy a reklámszünet rontja-e a platformszolgáltatás minőségét. A felhasználók ezt büntetésként élik meg, mert a reklámszünet zavarja a felhasználói élményt, és nyomásgyakorlás a hozzájárulás megadására. A Meta részéről is nehezen képzelhető el más üzleti érdek vagy motiváció, ugyanakkor érvelhet azzal, hogy a szolgáltatás ingyenes maradt, a Facebook funkciói továbbra is élnek.³³⁹ Véleményem szerint a Meta éppen azt valósítja meg, amit a DMA tilt, az 5. cikk (2) bekezdésben foglaltak kijátszását.

8. Összegzés és következtetés

A platformok több forrásból férnek hozzá a személyes adatokhoz: a felhasználók, a fogyasztók önként és aktívan adják át, ill. internetes nyomokat is hagynak, amelyek által szokásaik, viselkedésük megfigyelhetővé válik. Ezekből a nyomokból olyan következtetések is levonhatók, amelyek alapján csoportokba, kategóriákba sorolhatók. A kategorizálás negatív következményekkel járhat az érintettekre nézve (pl. pénzügyi szolgáltatások), de akár előnyt is hordozhat (pl. okosórák személyre szabott visszajelzései). A világhálón hagyott nyomokkal kapcsolatban a cookie-k és ezzel összefüggésben a fogyasztókról készített értékelések, vagyis a profilalkotás rejti a legtöbb veszélyt. A GDPR adatkezelésnek tekinti a profilalkotást, és biztosítja a tiltakozáshoz való jogot a felhasználónak. Előírja továbbá, hogy érthető, egyszerű nyelven kell tájékoztatást adni a személyes adatok kezelésére vonatkozó információkról. Ugyanakkor az szintén tény, hogy az érintetteknek kezelhetetlen mennyiségű online szerződést, szabályzatot és feltételt kell elolvasniuk és értelmezniük, de ha ezt még meg is teszik, az átlagfelhasználók – az információs aszimmetria miatt – a személyes adataik tekintetében nem tárgyalóképesek az adataikat kezelőkkel szemben.

³³⁸ DMA 13. cikk (6) bekezdés, (36)–(37) preambulumbekkezdés

³³⁹ EURÓPAI BIZOTTSÁG: *A Bizottság megállapítja...*

A tájékoztatás és az átláthatóság az online platformok használatát illetően tehát nem segíti a felhasználót a tájékozott döntés meghozatalában, amit a platformok üzleti modellje magyaráz. Egyik oldalon az egyre összetettebb technológia tudás, a másik oldalon a hosszú és érthetetlen tájékoztatók, ami tovább mélyíti az aszimmetriát. Ebből következően azt kell mondani, hogy a GDPR nem segíti a felhasználókat abban a döntési folyamatban, hogy hozzájáruljanak-e adataik kezeléséhez, vagy sem. A jogalkotó anélkül alkotott jogszabályt, hogy számolt volna az átlagfelhasználótól, az átlagfogyasztótól elvárható magatartással és informáltsággal, ezért szorgalmazták tanulmányok és fogyasztói szervezetek a digitális sérülékenységi fogalmának bevezetését. Az ezzel kapcsolatos DFA jogszabály javaslata 2026 végére készülhet el. Mindezek arra utalnak, hogy a személyes adatok védelme tekintetében szakadék tátong a platform és a felhasználó között. A szakadék okai: a profilalkotás, a cookie-k, az adatkezelési információk mennyisége, ill. a szolgáltató és a felhasználó aszimmetrikus információja, tudása. Mindezek azt eredményezik, hogy a felhasználók nincsenek tisztában személyes adataik értékével, és egyre kevésbé képesek rendelkezni azok felett; a platformok pedig kihasználják gyengeségeiket, és adataik felhasználásával befolyásolják őket.

A személyes adatok értékét vizsgálva tehát az adatvédelmi rendelkezéseken kívül szükségszerűen felmerülnek fogyasztóvédelmi kérdések is, ami azt mutatja, hogy e két terület közötti kapcsolat árnyalt és összetett. Szükséges, hogy megfelelő garanciák kerüljenek kiépítésre a jogrendszerben azért, hogy a gyengébb alkupozícióban lévő fél jogi érdekeinek védelme is érvényre jusson. A fogyasztók és platformok között kialakult egyensúlyhiányos helyzet kiegyenlítésén munkálkodik a fogyasztóvédelmi jog annak eszközrendszerével, a fogyasztóvédelem intézményrendszerének életre hívásával és a rá vonatkozó anyagi és eljárásjogi szabályok megalkotásával.³⁴⁰ (Részletezi a VI. fejezet.)

³⁴⁰ HAJNAL (2010) i. m. 15.

III. FEJEZET: AZ ÉRINTETTEK SZÁMÁRA BIZTOSÍTOTT VÉDELEM SZINTJE A SZEMÉLYES ADATAIK KEZELÉSE TEKINTETÉBEN – A GDPR

A személyes adatok kezelése tekintetében a természetes személyek védelmét szolgáló GDPR számtalan újdonságot hozott a korábbi adatvédelmi irányelvhez képest. Az újdonságok közül ebben a fejezetben több területre fókuszálok. Vizsgálom a területi hatályt és a végrehajtási kérdéseket. A végrehajtás tekintetében a határokon átnyúló egyablakos ügyintézési mechanizmusra koncentrálok, és kitekintek a GDPR eljárási rendeletére, amely 2027. április 2-ától alkalmazandó.³⁴¹ A fejezet fókuszában az érintettre vonatkozó jogok állnak, kiemelve azt, hogy a GDPR-ban az adatvédelmi irányelvhez képest milyen többletjogok jelennek meg. Az adatkezelés alapelvei közül két újdonságra világítok rá, a beépített és alapértelmezett adatvédelem alapelve, valamint az ehhez szorosan kapcsolódó elszámoltathatóság elvére; majd ezzel összefüggésben a GDPR által bevezetett új jogintézmény, az adatvédelmi hatásvizsgálat elemzése következik. Az érintetti jogok és az azokkal összefüggő alapelvek újszerűségének bemutatása azért nélkülözhetetlen, mert ezek a személyes adatok kezelése tekintetében a természetes személyek védelmét döntően meghatározó elemek, ebből következően a digitális gazdaság, az online platformok vonatkozásában további uniós jogi normák kiindulópontjaivá váltak, tehát előrejelzik, hogyan és miért fognak sarjadni a GDPR-ból további jogszabályok.

1. A GDPR és a tagállamok mozgástere

Az uniós adatvédelem egyik pillére a GDPR, amely – jogszabálytípusából következően – erős védelmet képes biztosítani az érintettek számára adataik kezelése tekintetében, mert közvetlenül alkalmazandó, ezáltal gátolja a korábbi irányelvi szabályozásból eredő tagállami széttagozottságot, jogbizonytalanságot. Az adatvédelmi szabályozás alapjait hordozó érintetti jogok és alapelvek tekintetében teljes harmonizáció valósul meg, de bizonyos területeken teret enged a tagállami szabályozásnak. Ezek egy része észszerű, hiszen a tagállami hagyományok és sajátosságok rugalmasabb szabályozást igényelnek. Az e dolgozat által érintett területek közül ilyen például az, hogy a levéltárak működése és szervezete különböző a tagállamokban, ezért a kapcsolódó garanciák sem lehetnek egységesek. Ebből következően a GDPR-t kiegészítik az archiválásra és a hozzáférésre vonatkozó nemzeti szabályok, Magyarországon ez az Infotv.-t és a levéltári törvényt³⁴² jelenti.

³⁴¹ Az Európai Parlament és a Tanács (EU) 2025/2518 rendelete (2025. november 26.) az (EU) 2016/679 rendelet végrehajtására vonatkozó további eljárási szabályok megállapításáról (a továbbiakban: GDPR eljárási rendelete)

³⁴² 1995. évi LXVI. törvény a köziratokról, a közlevéltárakról és a magánlevéltári anyag védelméről

Vannak azonban olyan területek, ahol nem értek egyet a tagállami szabadsággal, erre példa az, hogy az információs társadalommal összefüggő szolgáltatásokkal kapcsolatban a hozzájárulás érvényességéhez szükséges életkort a tagállamok 13–16 éves kor között állapíthatják meg. Véleményem szerint ez egységesítést igényelne, mert a digitális piac célkitűzéséhez jobban illeszkedne, a korhatárellenőrzés egyszerűsíthetőbb lenne, összességében tehát képes lenne hozzájárulni a széttöredezettség teljesebb felszámolásához.

2. A GDPR területi hatálya

Az adatvédelmi irányelvhez képest jelentős újdonságot hozott a GDPR a területi hatály tekintetében. A legfontosabb különbség a jogszabálytípusukból ered: az adatvédelmi irányelv alapján a tagállamok az implementált nemzeti rendelkezéseket alkalmazták, ezért először azt kellett megállapítani, hogy melyik tagállamnak a nemzeti joga a mérvadó a területi hatály tekintetében;³⁴³ a GDPR azonban – mivel rendelet – közvetlenül alkalmazandó.

A GDPR a területi hatályt illetően elkülöníti az EU-ban tevékenységi hellyel rendelkező és tevékenységi hellyel nem rendelkező adatkezelőket vagy adatfeldolgozókat. Előbbiek esetében a GDPR rendelkezéseit kell alkalmazni még abban az esetben is, ha maga az adatkezelés vagy -feldolgozás nem az EU területén történik.³⁴⁴ A tevékenységi hely tekintetében annak tisztázása fontos, hogy adott tevékenységet „tényleges és valós, tartós jelleget biztosító keretek” között gyakorolják-e, vagy sem; de a formának nincs jelentősége, lehet akár iroda, fióktelep stb.³⁴⁵ Lényegében ugyanezen ismérveket határozta meg az adatvédelmi irányelv,³⁴⁶ és az EUB a már korábban hivatkozott Weltimmo-ítéletében kimondta, hogy a tevékenység fogalma kiterjed minden, akár „csekély mértékű valós és tényleges tevékenységre, amelyet tartós jelleggel folytatnak.”³⁴⁷ Hasonló megállapítást tett a spanyol Google-ügyben hozott ítélet: az „egy szervezete tevékenységeinek keretében» kifejezést nem lehet megszorítóan értelmezni”³⁴⁸ az interneten kínált szolgáltatások esetében. Mindkét ítélet azt sugallja, hogy az EUB esetjoga tágan értelmezi a tevékenység és a tevékenységi hely fogalmakat, és már minimális érintettség esetén is alkalmazandónak tekinti a GDPR-t.

A GDPR területi hatályának megállapítása tekintetében a másik fontos szempont az, hogy ha az EU-ban tevékenységi hellyel nem rendelkezik az adatkezelő vagy az adatfeldolgozó,

³⁴³ Adatvédelmi irányelv 4. cikk

³⁴⁴ GDPR 3. cikk (1) bekezdés

³⁴⁵ GDPR (22) preambulumbekkezdés

³⁴⁶ Adatvédelmi irányelv (19) preambulumbekkezdés

³⁴⁷ EUB-ítélet C-230/14. ügy 31–32. pont

³⁴⁸ ECLI:EU:C:2014:317. A Bíróság (nagytanács) ítélete a C-131/12. sz. ügyben (spanyol Google és Mario Costeja González), 2014. május 13. (a továbbiakban a lábjegyzetekben: EUB-ítélet C-131/12. sz. ügy) 53. pont

de az ott tartózkodó érintettek személyes adatainak a kezelését végzi, akkor e tevékenységek mihez kapcsolódnak: áruk és/vagy szolgáltatások nyújtásához, avagy az érintettek viselkedésének megfigyeléséhez. Az áruk és szolgáltatások nyújtása tekintetében teljesen mindegy, hogy kell-e ezekért fizetni, vagy sem.³⁴⁹ A viselkedés megfigyeléséhez kapcsolódást nevezi az EDPB megcélzásnak. A megcélzást láttatja az alábbi példa: egy törökországi honlap családi fényképalbumok készítésére vonatkozó szolgáltatásokat kínál, amely angol, francia, holland és német nyelven érhető el; és a kész albumokat postázzák Franciaországba, a Benelux-államokba és Németországba. Ez utóbbiak azt jelentik, hogy adott szolgáltatást az EU-n belül kínálják, uniós fogyasztókat céloznak. A honlap adatkezelőként végez adatkezelést, ami a szolgáltatás EU-n belüli érintetteknek történő nyújtásához kapcsolódik,³⁵⁰ tehát vonatkoznak rá a GDPR-kötelezettségek.³⁵¹ Ebben az esetben a honlapnak uniós képviselőt kell kijelölnie.³⁵² A példa adatvédelmi és fogyasztóvédelmi szempontból is ugyanahhoz az eredményhez vezet: az uniós fogyasztók kiszolgálása önmagában megalapozza az uniós jog alkalmazását.

A GDPR-t akkor is alkalmazni kell, ha az érintettek EU-n belüli viselkedésének megfigyeléséhez kapcsolódik a tevékenység. Bár ez internetes nyomon követést jelent,³⁵³ „a más jellegű hálózatokon vagy technológiákkal – például viselhető és egyéb intelligens eszközökkel – folytatott, személyes adatok kezelésével járó nyomon követést is figyelembe kell venni annak megállapításához, hogy egy adott adatkezelési tevékenység viselkedés megfigyelésének minősül-e.”³⁵⁴ Itt a megfigyelés szó jelentéséből kiindulva az adatkezelés célját, valamint az adatok felhasználására alkalmazott viselkedéselemzési vagy profilalkotási technikákat kell szem előtt tartani. Az EDPB szerint különösen ide tartoznak az alábbi tevékenységek: viselkedésalapú hirdetés; földrajzi helymeghatározás (marketingcélokra); nyomon követés cookie-kkal, nyomkövető technikákkal, például ujjnyomátvétellel; zártláncú televíziós rendszer; piacfelmérés egyéni profilok alapján; egészségi állapot megfigyelése.³⁵⁵

Ha az EU-ban tevékenységi hellyel nem rendelkező adatkezelő vagy adatfeldolgozó az EU-ban tartózkodó érintettek személyes adatait kezeli (akár termékek, szolgáltatások kínálásához, akár magatartásuk megfigyeléséhez kapcsolódóan), akkor a GDPR alapján uniós képviselőt kell kijelölnie írásban.³⁵⁶ A képviselő feladata az, hogy az adatkezelő vagy az

³⁴⁹ GDPR 3. cikk (2) bekezdés

³⁵⁰ EDPB: 3/2018. sz. iránymutatás az általános adatvédelmi rendelet területi hatályáról (3. cikk) 2.1 változat. 2019. november 12. 21. 14. példa

³⁵¹ GDPR 3. cikk (2) bekezdés a) pont

³⁵² GDPR 27. cikk

³⁵³ GDPR (24) preambulumbekkezdés

³⁵⁴ EDPB: 3/2018. 22.

³⁵⁵ EDPB: 3/2018. 23.

³⁵⁶ GDPR 27. cikk és (80) preambulumbekkezdés

adattfeldolgozó nevében eljárjon a GDPR értelmében fennálló kötelezettségek tekintetében – ami nem érinti az említett rendeletből következő hatásköröket és felelősséget –, konkrétan ez azt jelenti, hogy az illetékes felügyeleti hatóság és az érintettek szükség esetén a képviselőt fogják keresni, mint az adatkezelő kapcsolattartóját.³⁵⁷ Ebből az is következik, hogy a képviselő nevét és elérhetőségeit közzé kell tenni, valamint hogy az EU-ban tevékenységi hellyel kell rendelkeznie. Általában ügyvédi irodák, tanácsadó cégek töltik be e szerepkört, de nem tölthetik be külső adatvédelmi tisztviselők.³⁵⁸

A GDPR kiterjesztett, széles területi hatálya nem egyedi jellemző, előképe az EU több fogyasztóvédelmi jogszabályában tetten érhető. A Brüsszel Ia. rendelet kimondja, hogyha a kereskedelmi vagy szakmai tevékenység „bármilyen módon az említett tagállamra [...] irányul,”³⁵⁹ akkor a fogyasztó a saját lakóhelye szerinti bírósághoz fordulhat. Hasonlóan fogalmaz a Róma I. rendelet is, amely alapján a fogyasztói szerződésekre „annak az országnak a joga az irányadó, ahol a fogyasztó szokásos tartózkodási helye található, feltéve, hogy a vállalkozó [...] tevékenységei ebbe az országba [...] irányulnak.”³⁶⁰ A tevékenység irányulása a GDPR megfogalmazásában úgy hangzik, hogy „az érintettek viselkedésének megfigyeléséhez” kapcsolódik, tehát nem a vállalkozás letelepedési helyét, hanem a fogyasztó megcélzását tekinti fő szempontnak, azaz a fogyasztóvédelmi uniós jogszabályok gyengébb fél védelmén alapuló, fogyasztóközpontú megközelítését követi. Az időben későbbi DSA töretlenül folytatja ezt a szemléletet, és szinte megismétli a GDPR kulcsszavait: minden olyan közvetítő szolgáltatásra kiterjeszti hatályát, amelyet az Unióban letelepedett vagy ott tartózkodó igénybevevőknek nyújtanak, „függetlenül a [...] szolgáltatók letelepedési helyétől.”³⁶¹ (Ugyanígy a digitális piacokról szóló DMA is a végfelhasználók helyzetére összpontosít, és a részükre kínált alapvető platformszolgáltatásokra vonatkozik, „függetlenül a kapuőrök székhelyétől vagy tartózkodási helyétől.”)³⁶² Véleményem szerint a fenti párhuzamok azt mutatják, hogy területi hatály tekintetében a fogyasztóvédelmi jogszabályok és a GDPR egymást erősítik: a következetes fogyasztóközpontú szemlélet védőhálót képez az egységes piacon a fogyasztók köré az adatvezérelt gazdasági szereplőkkel szemben; ugyanakkor azt is

³⁵⁷ GDPR (80) preambulumbekkezdés

³⁵⁸ EDPB: 3/2018. 27.

³⁵⁹ Az Európai Parlament és a Tanács 1215/2012/EU rendelete (2012. december 12.) a polgári és kereskedelmi ügyekben a joghatóságról, valamint a határozatok elismeréséről és végrehajtásáról (a továbbiakban: Brüsszel Ia. rendelet) 17. cikk (1) bekezdés c) pont

³⁶⁰ Az Európai Parlament és a Tanács 593/2008/EK rendelete (2008. június 17.) a szerződéses kötelezettségekre alkalmazandó jogról (a továbbiakban: Róma I. rendelet) 6. cikk (1) bekezdés

³⁶¹ DSA 2. cikk (1) bekezdés

³⁶² DMA 1. cikk (2) bekezdés

meg kell jegyezni, hogy ez a háló mindaddig nem válik páncéllá, amíg az uniós képviselő intézményének korlátozott kikényszeríthetősége nehezíti a jogérvényesítést.

3. A GDPR végrehajtása: a felügyeleti hatóságok

A felügyeleti hatóságok független jogállásúak, ami egyrészt személyi, másrészt szervezeti függetlenséget jelent. A személyi függetlenség szakmai és szűkebb értelemben vett személyi függetlenséget (tagjait átlátható eljárásban nevezi ki a GDPR-ban meghatározott jogosultak egyike; képesítés, tapasztalat megléte; hivatalukból nem mozdíthatók el³⁶³) jelent; a szervezeti függetlenség horizontális és vertikális függetlenséget jelent. A szervezeti függetlenség részeként fontos szerep jut annak, hogy a feladataik ellátásához szükséges emberi, műszaki, pénzügyi erőforrásokat, helyiségeket és infrastruktúrát biztosítani kell számukra.³⁶⁴

3.1. Az egyablakos ügyintézési mechanizmus

Az adatvédelmi irányelv és a GDPR közötti legjelentősebb eltérés abból a jogalkotói szándékból ered, hogy míg korábban, az irányelv hatálya alatt a tagállami hatóságok önálló és a többi hatóságtól elszigetelt eljárást folytattak, az együttműködésre vonatkozó konkrét szabályok nélkül, addig a GDPR elvárja, hogy az EU-ban teljesen egységesen kezeljék az adatvédelmi ügyeket, értelmezzék és alkalmazzák a rendeletet,³⁶⁵ ezért a felügyeleti hatóságok számára együttműködési kötelezettséget és egységességi mechanizmust ír elő, amelyet különösen akkor kell alkalmazni, ha több tagállam nagyszámú érintettjét jelentős mértékben érintő adatkezelés a vizsgálat tárgya.³⁶⁶ Ha valamely tagállam több felügyeleti hatóságot hozott létre,³⁶⁷ ezek közül ki kell jelölnie azt az egyet, amelyik az EDPB-ben képviseli a többi hatóságot, valamint részt vesz az egységességi mechanizmusban.³⁶⁸ Ezáltal biztosítható az, hogy a határon átnyúló ügyekben „egy hatóságként járnak el az adatkezelővel szemben,

³⁶³ Magyarország 2012. január 1-jével – az Infotv. hatályba lépésével párhuzamosan – mandátumának letelte előtt megszüntette a személyes adatok védelmét felügyelő hatóság megbízatását, az EUB ítélete szerint ez azt jelenti, hogy nem teljesítette az adatvédelmi irányelvből eredő kötelezettségeit. ECLI:EU:C:2014:237. A Bíróság ítélete (nagytanács) a C-288/12. sz. ügyben (Bizottság kontra Magyarország), 2014. április 8. 67. pont

³⁶⁴ PÉTERFALVI Attila – RÉVÉSZ Balázs – BUZÁS Péter (szerk.): *Magyarázat a GDPR-ról*. Bp., Wolters Kluwer Hungary, 2021. 396–400.

³⁶⁵ GDPR 51. cikk (2) bekezdés

³⁶⁶ GDPR (135) preambulumbekkezdés és 63. cikk

³⁶⁷ Magyarországon egyetlen felügyeleti hatóságot állítottak fel, a NAIH-t, de néhány tagállamban többet is, így pl. Németországban, ahol a szövetségi rendszer indokolja az egynél több hatóság működését.

³⁶⁸ GDPR (119) preambulumbekkezdés, 51. cikk (3) bekezdés

kijelölve maguk közül a fő felügyeleti hatóságot és az érintett hatóságokat,”³⁶⁹ vagyis ún. egyablakos ügyintézési mechanizmusnak (one-stop-shop) kell érvényesülnie.³⁷⁰

Az egyablakos ügyintézési eljárás előnyös az adatkezelők számára, mert csak egy tagállam felügyeleti hatóságával kell együttműködniük, de számtalan kérdést fölvet a fő felügyeleti hatóság és az érintett hatóság(ok) szempontjából. Ilyen kérdés az – ami az egyablakos ügyintézési eljárás megindításához elengedhetetlenül fontos –, hogy mely tagállam hatósága illetékes fő felügyeleti hatósággént eljárni, és melyek lesznek az érintett hatóságok. Alapvetően figyelemmel kell lenni arra, hogy fő felügyeleti hatósággént az adatkezelő/adatfeldolgozó tevékenységi központja vagy egyetlen tevékenységi helye szerinti felügyeleti hatóság jogosult eljárni; és érintett az a hatóság lehet, amelynek tagállamában szintén van tevékenységi helye az adatkezelőnek/adatfeldolgozónak, vagy jelentős mértékben érintettek a tagállamban letelepedett természetes személyek, vagy panasz érkezett hozzá.³⁷¹ Előfordulhatnak azonban olyan esetek, amikor a fentiek alapján több felügyeleti hatóság is szóba jöhet, ezek közül az lesz illetékes, amelynek tagállamában a döntést meghozzák az adatkezelési tevékenységről.³⁷² Továbbá felmerülhet az is, hogy az illetékesség tekintetében változás következik be, például a vállalat a tevékenységi központját áthelyezi egyik tagállamból a másikba, e kérdésben az EDPB állásfoglalása egyértelmű: a jogerős döntés meghozataláig az illetékesség átszállhat egyik hatóságról a másikra.³⁷³

A határokon átívelő ügyekben az egyablakos ügyintézési eljárás mechanizmusa több lépésből áll.³⁷⁴ Az első lépés a releváns információk megosztása egymással. A fő felügyeleti hatóság bármikor kérhet az érintett hatóságoktól kölcsönös segítségnyújtást és végezhet közös műveleteket.³⁷⁵ A következő lépésben elkészül a fő felügyeleti hatóság döntéstervezete. Ezt követően két forgatókönyv lehetséges: ha az érintett felügyeleti hatóságok nem emelnek kifogást (négy héten belül), a döntés elfogadottnak tekinthető, és lezárul az eljárás; ha azonban kifogást emelnek, azt meg kell vizsgálnia a fő felügyeleti hatóságnak. Ebben az esetben két alternatívával lehet számolni: a kifogást vagy nem tartja elfogadhatónak, relevánsnak és megalapozottnak, vagy nem ért vele egyet, ezekben az esetekben az ügy vitás kérdéseit az EDPB elé utalja; vagy egyetért a kifogásokkal, s ezt figyelembe véve módosítja

³⁶⁹ PÉTERFALVI–RÉVÉSZ–BUZÁS i. m. 395.

³⁷⁰ GDPR 56. cikk (1) bekezdés

³⁷¹ GDPR 56. cikk

³⁷² PÉTERFALVI–RÉVÉSZ–BUZÁS i. m. 412.

³⁷³ EDPB: 8/2019. számú vélemény a felügyeleti hatóságnak a tevékenységi központhoz vagy az egyetlen tevékenységi helyhez kapcsolódó körülmények megváltozása esetén fennálló illetékességről. Elfogadva 2019. július 9-én. 30. pont

³⁷⁴ GDPR 60. cikk

³⁷⁵ GDPR 61–62. cikk

döntéstervezetét, és újra elküldi az érintett hatóságoknak. Ebben az esetben az érintett felügyeleti hatóságok (két hét alatt) ellenőrzik, és újra kétféle lehetőséggel kell számolni: vagy nem emel kifogást egyetlen érintett hatóság sem, ez esetben a döntés rájuk nézve kötelező; vagy egyet nem értés esetén a fő felügyeleti hatóság az ügyet az EDPB elé utalja, vitarendezési eljárás lefolytatására.

A teljes folyamatban kulcsfontosságú elem a konszenzusra törekvés,³⁷⁶ ezért előbb az együttműködési mechanizmus valamennyi eszközét (a vizsgálati szakaszban: folyamatos információcsere, megkeresések, kölcsönös segítségnyújtás, közös műveletek, például helyszíni ellenőrzés) ki kell meríteni, s csak ez után kerülhet sor az egységességi mechanizmus keretében való kezelésre,³⁷⁷ ami azt jelenti, hogy az EDPB kötelező erejű döntést fogad el.³⁷⁸

Az egyablakos ügyintézési eljárással kapcsolatban a belga fellebbviteli bíróság³⁷⁹ (is) felhívta a figyelmet arra a köztudott problémára, hogy Írországból van az európai központja több amerikai online óriáscégnek, például a Facebooknak, Apple-nek és a Google-nak – kihasználva „a szabályozási arbitrázsban rejlő lehetőségeket, vagyis amikor a gazdasági társaság az enyhébb szabályozási környezetet biztosító országot választja székhelyéül,” ami „a digitalizációban érintett szolgáltatók esetében is felveti a könnyebb ellenállás felé vezető út aktív keresését”³⁸⁰ –, így e vállalkozások adatkezelői vonatkozásában az ír adatvédelmi hatóság fog eljárni mint fő felügyeleti hatóság. Mivel a panaszok nagy része e vállalatokkal szemben érkezik, gyakorlatilag egyetlen nemzeti adatvédelmi hatóságnál koncentrálódnak a nagy ügyek, ami már önmagában is hátráltatja a GDPR végrehajtását. További problémát jelent az, hogy Írország nemcsak adópolitikájával³⁸¹ kedvez e nagyvállalatoknak, hanem az adatvédelmi hatósága teljesítménye tekintetében a leggyengébb láncszem Európában,³⁸² ezért még kötelezettségszegési eljárás indítása is szóba került ellene.³⁸³ A vállalatok a forum shopping

³⁷⁶ EDPB: 02/2022. sz. iránymutatás az általános adatvédelmi rendelet 60. cikkének alkalmazásáról. 1.1. verzió. Elfogadva: 2022. március 14. 149. pont

³⁷⁷ EDPB: 02/2022. 117. pont

³⁷⁸ GDPR 65. cikk (1) bekezdés

³⁷⁹ ECLI:EU:C:2021:483. A Bíróság ítélete (nagytanács) a C-645/19. sz. ügyben (belga adatvédelmi hatóság kontra Facebook), 2021. június 15. (a továbbiakban a lábjegyzetekben: EUB-ítélet C-645/19. sz. ügy)

³⁸⁰ GLAVANITS Judit: *A gazdasági folyamatok digitalizációjának egyes biztonsági és szabályozási kérdései*. Military and Intelligence CyberSecurity Research Paper 2023/6. 12.

³⁸¹ TÓTH András: *Az adatmonopóliumok tündöklése és letörése*. In: SZABÓ Endre Győző: *Az Infotörvénytől a GDPR-ig*. Bp., Ludovika Egyetemi Kiadó, 2021. 172.

³⁸² Madhumita MURGIA – Javier ESPINOZA: *Ireland is 'worst bottleneck' for enforcing EU data privacy law – ICCL Report says Irish data protection watchdog failing to take action against US tech giants*. 2021. szeptember 13. <https://www.irishtimes.com/business/technology/ireland-is-worst-bottleneck-for-enforcing-eu-data-privacy-law-iccl-1.4672480> (letöltés: 2023. 02. 02.). Írország 2020-ig 196 ügyből csak négyet zárt le, és nem nyújtott be határozattervezeteket határokon átnyúló ügyekben.

³⁸³ P9_TA(2021)0256. European Parliament: 2019-2024:Texts Adopted. 4–5. pont. https://www.europarl.europa.eu/doceo/document/TA-9-2021-0256_EN.pdf (letöltés: 2025. 01. 03.)

eszközével élve enyhébb szankciókra számíthatnak³⁸⁴ – ami akár tevékenységiközpont-áthelyezési lavinát indíthat el –, erre utal az EUB-ítélet is: „az »egyablakos ügyintézési« mechanizmus semmi esetre sem eredményezheti azt, hogy valamely nemzeti felügyeleti hatóság, különösen a fő felügyeleti hatóság ne lássa el a rá háruló feladatokat, mert ellenkező esetben a forum shopping gyakorlatát ösztönözné.”³⁸⁵ Az utóbbi pár évben azonban mind az adózást illetően,³⁸⁶ mind a hatóság hatékonyságát illetően³⁸⁷ történt némi pozitív elmozdulás.

3.2. A GDPR eljárási rendelete

Sok kritika éri a GDPR decentralizált végrehajtási modelljét mind a tagállami felügyelő hatóságok, mind nemzetközi szervezetek részéről, amelyek többek között azt nehezményezik, hogy a digitális nagyvállalatokat érintő esetekkel az egyablakos ügyintézési mechanizmus keretében csak egy hatóság foglalkozik mindaddig, amíg a döntési szakaszba nem ér az ügy, ami lassítja a folyamatokat, és megállapítják, hogy a hatékonyságot az biztosítaná, ha a végrehajtás ugyanolyan központosított lenne, mint a DMA vagy a DSA esetében.³⁸⁸ A problémákat elismerik a GDPR alkalmazását értékelő bizottsági közlemények is,³⁸⁹ s bár nincs tervbe véve a teljes jogszabályi felülvizsgálat, de a határokon átnyúló ügyek hatékonyabb és harmonizált kezelése érdekében megszületett a GDPR eljárási rendelete.

E rendelet nem változtat az egyablakos ügyintézési kereteken, és csak a határokon átnyúló ügyekben állapít meg egységes eljárási szabályokat. Előírja, hogy a panasznak milyen információkat kötelező tartalmaznia, és rögzíti, hogy a harmonizált kritériumokon kívül a hatóságok nem kérhetnek több adatot a befogadhatósághoz.³⁹⁰ Új jogintézményként bevezeti a korai szakaszban történő rendezés lehetőségét, ezzel lehetővé teszi a panasz gyorsabb, egyszerűsített rendezését még a teljes eljárás megindítása előtt (pl. ha a vállalat már orvosolta

³⁸⁴ SZEGEDI László – DORNFELD László – POLGÁR Zoltán – TELEKI Bálint: *A GDPR alkalmazásával kapcsolatos első tagállami tapasztalatok – Egységes szabályozás, eltérő alkalmazás?* Infokommunikáció és Jog 2021/1. 10.

³⁸⁵ EUB-ítélet C-645/19. sz. ügy 68. pont

³⁸⁶ BOLCSÓ Dániel: *Évtizedes vita ért véget: az Apple-nek gigantikus adóhátralékot kell fizetnie az EU-ban.* 2024. szeptember 10. <https://telex.hu/gazdasag/2024/09/10/apple-europai-unio-birosaga-13-milliard-euro-birsag-adozas-irorszag> (letöltés: 2024. 10. 02.); KOI Tamás: *Írország elfogadja a globális minimumadót.* Hír, 2021. október 8. <https://www.hsw.hu/hirek/63844/irorszag-g20-oecd-tarsasagi-ado.html> (letöltés: 2024. 10. 02.)

³⁸⁷ KOZMA Zoltán – ALMÁSY Márk: *Közel 6 milliárd euró bírság a GDPR óta.* Blogbejegyzés 2025. 01. 29. <https://blogs.dlapiper.com/advocatus/2025/01/kozel-6-milliard-euro-birsag-a-gdpr-ota/> (letöltés: 2025. 02. 13.)

³⁸⁸ Matt BURGESS: *How GDPR Is Failing.* <https://www.wired.com/story/gdpr-2022/> (letöltés: 2023. 03. 03.)

³⁸⁹ COM(2020) 264 final. A Bizottság közleménye az Európai Parlamentnek és a Tanácsnak: A polgárok szerepe erősítésének és az EU digitális átállással kapcsolatos megközelítésének pillérét képező adatvédelem – az általános adatvédelmi rendelet alkalmazásának két éve. Brüsszel, 2020. 06. 24.; COM(2024) 357 final. A Bizottság közleménye az Európai Parlamentnek és a Tanácsnak: Második jelentés az általános adatvédelmi rendelet alkalmazásáról. Brüsszel, 2024. 07. 25.

³⁹⁰ GDPR eljárási rendelete 4. cikk

a jogsértést, a panasz oka fogyottá vált).³⁹¹ A GDPR 60. cikke (1) bekezdésének értelmében vett konszenzus elérése érdekében a fő felügyelő hatóságokra telepíti a részletesen felsorolt releváns információkról való tájékoztatási kötelezettséget az érintett hatóságok számára; előzetes véleménye kialakítása után a legfontosabb kérdések összefoglalójának elkészítését.³⁹² Hangsúlyozza az észszerű határidők tartását, és konkrét határidőket is meghatároz – mely mérhetőséget és a számonkérhetőséget is jelent –, így például a fő felügyeleti hatóságnak főszabály szerint 15 hónapon belül elő kell terjesztenie a döntéstervezetét.³⁹³ Továbbá a vizsgálat alá vontak számára garanciajellegű eljárási jogokat biztosít, különösen a meghallgatáshoz való jog terjedelmét és az iratbetekintési jogot illetően.³⁹⁴

A GDPR eljárási rendelete új eljárási szabályainak az lesz a legfontosabb előnye – véleményem szerint –, hogy konkrét és észszerű határidők meghatározása által a jogérvényesítésre nem kell majd évtizedeket várni. Az elhúzódó eljárások kiüresítik a jogérvényesítést, sőt ezáltal a vállalkozások versenyelőnyre tehetnek szert, vagy megerősíthetik azt. Kérdéses azonban, hogy a digitális nagyvállalatokkal kapcsolatos ügyekre vonatkozóan tarthatók-e ezek a határidők, erre a GDPR eljárási rendeletének preambuluma is utal: az észszerű határidő „az egyes ügyek körülményeitől és különösen azok kontextusától [...], az ügy összetettségétől függ.”³⁹⁵ Ezzel kapcsolatban természetesen az is elgondolkodtató, hogy biztosított lesz-e hozzá az emberi erőforrás és a működési kapacitás. Hatványozottan merül föl ez a kérdés az ír adatvédelmi hatóság tekintetében, amelyet sok kritika ért a lassúsága miatt, ugyanakkor az éves jelentésükben emelkedő számú lezárt ügyről, növekvő költségvetésről, folyamatos létszámnövekedésről és szakmai képzésről számolnak be.³⁹⁶ A panaszbefogadhatóság harmonizált feltételeinek meghatározása az érintetti pozíció erősítését szolgálja. Idekapcsolódik az is, hogy a fogyasztóvédelmi szervezetek gyakran szembesülnek azzal a problémával, hogy minden tagállamban más szabályok szerint kell beadniuk a panaszt. A GDPR eljárási rendelete lehetővé teszi, hogy például a BEUC a fogyasztók széles körét érintő adatvédelmi ügyekben könnyebben tudjon eljárni. Ugyanakkor az is kérdéses, hogy egy

³⁹¹ GDPR eljárási rendelete 5. cikk

³⁹² GDPR eljárási rendelete 9–10. cikk

³⁹³ GDPR eljárási rendelete 12. cikk

³⁹⁴ GDPR eljárási rendelete 19., 22. és 24. cikk

³⁹⁵ GDPR eljárási rendelete (17) preambulumbekkezdés

³⁹⁶ DATA PROTECTION COMMISSION: *Annual Report 2023*. 24–25., 90. https://www.dataprotection.ie/sites/default/files/uploads/2024-05/DPC%20EN_AR%202023_Final%20.pdf (letöltés: 2025. 12. 03.); DATA PROTECTION COMMISSION: *Annual Report 2024*. 28., 110. https://www.dataprotection.ie/sites/default/files/uploads/2025-06/DPC_Annual_Report_EN_Low_Res.pdf (letöltés: 2025. 12. 03.)

magánszemély ismer-e minden, az adatkezelőre vonatkozó adatot,³⁹⁷ s ha nem, a hatóságok nem fogják-e a panaszt elutasítani. Az eljárás tisztességessége érdekében a jogalkotó a vizsgálat alá vontak számára is garanciális jogokat biztosít, de mivel ezek erősítik a nagyvállalatok pozícióját az egyéni érintettekkel szemben, ezért alkalmasak lehetnek az eljárás nyújtására is, ami ronthatja a két fél egyensúlyát.

A GDPR eljárási rendelete a fogyasztóvédelmi eszközökkel több kapcsolódási pontot mutat. Alapvetően mindkettő növeli a hatékonyságot, de úgy, hogy közben egyik sem számolja fel teljesen a tagállami hatóságok szerepét. A korai szakaszban történő rendezés jogintézménye párhuzamba állítható a fogyasztóvédelemben alkalmazott alternatív vitarendezési mechanizmusokkal (békéltető testület; online vitarendezési platform, 2025-ben megszűnt), mindkettő célja a gyors, olcsó és rugalmas megoldás, ami várhatóan elősegíti majd a hatóságok tehermentesítését. A panaszbefogadhatóság kritériumainak meghatározása, valamint hogy más adat nem kérhető a panasz befogadásához, emlékeztet a fogyasztóvédelemben egyre hangsúlyosabb alacsony küszöbértékű jogérvényesítés elvére.³⁹⁸

4. Az érintettek jogai a GDPR alapján

4.1. Átlátható tájékoztatás és a tájékoztatáshoz való jog

A személyes adatok kezelésének jogszerűnek, tisztességesnek és az érintettek számára átláthatónak kell lennie, abban a tekintetben, hogy a rájuk vonatkozó személyes adatokat hogyan gyűjtik és használják fel; azokba hogy tekintenek bele vagy milyen egyéb módon kezelik; milyen mértékben kezelik vagy fogják kezelni.³⁹⁹

A GDPR három alapelvet emel ki a tájékoztatással kapcsolatban, ezek közül a jogszerűség és a tisztességesség már az adatvédelmi irányelvben⁴⁰⁰ is szerepelt, az átláthatóság azonban új fogalomként jelent meg a rendeletben. Az átláthatóság célja, hogy bizalmat alakítson ki a polgároknál azáltal, hogy a folyamatokat megértetik velük, és szükség esetén az

³⁹⁷ GDPR eljárási rendelete 4. cikk (1) bekezdés d) pont: a panasz tárgyát képező adatkezelő vagy adatfeldolgozó azonosítását elősegítő információk

³⁹⁸ Célja az, hogy az egyéni jogérvényesítés ne járjon aránytalan terhekkel, ezért olcsó, gyors jogérvényesítést tesz lehetővé a fogyasztó számára, azon gátak jogszabályi lebontásával, amelyek eltántorítanák a jogérvényesítéstől (pl. pénzügyi [ingyenes], eljárási [egyszerű formanyomtatvány] és bizonyítási [valamely hivatal vagy szervezet jár el, és gyűjti össze a bizonyítékokat] küszöb megszüntetése). Néhány vonatkozó rendelkezés: képviseleti keresetekről szóló irányelv 20. cikk; UCP-irányelv 11a. cikk; Fgy. tv. 18. § (1) bekezdés, 25. § (1) bekezdés, 36/C §.

³⁹⁹ GDPR (39) preambulumbekkezdés

⁴⁰⁰ Adatvédelmi irányelv II. fejezet és 6. cikk (1) bekezdés

azokkal szembeni tiltakozást lehetővé teszik;⁴⁰¹ ugyanakkor szorosan összefügg a tisztességes eljárás és az adatkezelőre vonatkozó elszámoltathatóság követelményével.⁴⁰² Az átláthatóság követelményei három szempont mentén csoportosíthatók. Egyrészt fontos a három alkalmazási területe: a tisztességes adatkezeléssel kapcsolatos tájékoztatás nyújtása az érintettek részére; tájékoztatásuk a GDPR szerinti jogaikkal kapcsolatban; és jogaik gyakorlásának megkönnyítése az adatkezelők által. Másrészt fontos az, hogy a teljes adatkezelési időtartam mely szakaszára terjed ki: az adatgyűjtés időszakára; a teljes adatkezelési időszakra; valamint az adatkezelés valamely kiemelt pontján (pl. adatvédelmi incidens esetén). Az érintettek jogaira vonatkozóan megkülönböztethetők: az érintettek rendelkezésére bocsátott információk,⁴⁰³ amelyek alapján összefoglaló, átfogó tájékoztatást nyújtanak a személyes adataik kezeléséről; tájékoztatásuk a jogaik gyakorlásával kapcsolatban;⁴⁰⁴ valamint az adatvédelmi incidensekkel kapcsolatosan.⁴⁰⁵

Az érintettek tájékoztatásának és a kommunikációnak minden területére érvényesek az átláthatósággal kapcsolatos, a tájékoztatás érthetőségét, értelmezhetőségét támogató elvárások, amelyek főleg a nyelvi megformáltságra vonatkoznak. A tájékoztatás legyen:⁴⁰⁶ tömör, átlátható és érthető, azaz a célcsoport átlagos tagjának meg kell értenie.⁴⁰⁷ Fontos követelmény a világos és közérthető nyelvezet; ez a követelmény a gyermekeknek szóló információk tekintetében kiegészül azzal, hogy a szókincs és a stílus is gyermekközpontú legyen, még akkor is, ha a hozzájárulást a szülő adja meg, hiszen a célcsoportot a gyermekek jelentik. A tájékoztatás írásban vagy más módon – ideértve az elektronikus utat is – adható, sőt engedélyezett ikonokkal és jelölésekkel⁴⁰⁸ is ellátni a tájékoztatást, de ezek nem helyettesíthetik a szöveges tájékoztatást, és géppel olvasható formátumúnak kell lenniük.⁴⁰⁹ A tájékoztatás a nyelvi minőségen túl legyen könnyen hozzáférhető (keresés nélkül azonnal észrevehető), és legyen díjmentes (általában).⁴¹⁰

⁴⁰¹ WP260. A 29. cikk szerinti munkacsoport: Iránymutatás az (EU) 2016/679 rendelet szerinti átláthatóságról. 4–5.

⁴⁰² GDPR 5. cikk (1) bekezdés a) pont és 5. cikk (2) bekezdés

⁴⁰³ GDPR 13–14. cikk

⁴⁰⁴ GDPR 15–22. cikk

⁴⁰⁵ GDPR 34. cikk

⁴⁰⁶ GDPR 12. cikk (1) bekezdés

⁴⁰⁷ WP260. 7–8.

⁴⁰⁸ GDPR (60) preambulumbekkezdés

⁴⁰⁹ Egy dokumentum akkor olvasható számítógéppel, ha olyan fájlformátumú, amely lehetővé teszi a szoftveres alkalmazások számára, hogy a benne lévő egyedi adatokat könnyen azonosítsák, felismerjék és kinyerjék. A számítógéppel olvasható formátumban létrehozott fájlokban kódolt adatok számítógéppel olvasható adatoknak tekintendők. Az Európai Parlament és a Tanács 2013/37/EU irányelve (2013. június 26.) a közzféra információinak további felhasználásáról szóló 2003/98/EK irányelv módosításáról (21) preambulumbekkezdés

⁴¹⁰ GDPR 12. cikk (5) bekezdés

A hogyan adjanak az adatkezelők tájékoztatást kérdéskörébe tartozó elvárások, szabályok mellett a mit, miről kell tájékoztatást adni kérdésre is válaszolnunk kell, azaz hogy minimálisan mely adatkezelési körülményekről kell az adatkezelőknek tájékoztatniuk az érintetteket. Erre a kérdésre a Rendelkezésre bocsátandó információk⁴¹¹ cím alatt találunk választ. Akár az érintettől szerzik, akár nem az érintettől szerzik a személyes adatokat, szükséges tájékoztatni az érintetteket: az adatkezelő és az adatvédelmi tisztviselő elérhetőségéről; az adatkezelés céljáról, jogalapjáról, az adattárolás időtartamáról; az érintetti jogokról; valamint a felügyeleti hatósághoz címzett panasz benyújtásának jogáról. Ezeken túlmenően, ha releváns, akkor tájékoztatást kell nyújtani arról is, hogy az adatokat kinek adják át, s ha ez harmadik ország vagy nemzetközi szervezet, a megfelelő garanciákról is; valamint az automatizált döntéshozatallal összefüggő információkról. Ha a személyes adatokat nem az érintettől szerzik, a fentiekén túl a következőkről is tájékoztatást kell nyújtani: a személyes adatok forrása (harmadik fél adatkezelők, nyilvánosan elérhető források, adatbrókerek vagy egyéb érintettek⁴¹²), és hogy ezek nyilvánosan hozzáférhető forrásból származnak-e. Az érintettek rendelkezésére bocsátandó információkon kívül a GDPR előírja az érintettek tájékoztatási kötelezettségét a jogaik gyakorlásával kapcsolatban is,⁴¹³ amellyel az érintettek ténylegesen olyan helyzetbe kerülnek, hogy képesek lesznek jogaik érvényesítésére.⁴¹⁴

A fentiek alapján azt látjuk, hogy a GDPR alapján mérhetetlen mennyiségű információról kell az adatkezelőnek tájékoztatást nyújtani az érintettek számára, ami szemben áll a tömörség és az érthetőség követelményével, s ezt a szembenállást nem fogja feloldani az átláthatóság követelménye. A jogalkotók az információs aszimmetriát ellensúlyozó varázsszerként tekintenek az átláthatóságra, napjainkra azonban – véleményem szerint – éppen ez a vonása vált ellentmondásossá. Erősségei (tudatos döntéshozatal, önrendelkezés) hordozzák a gyengeségeit: a hosszú és érthetetlen adatkezelési tájékoztatók formálisan teljesítik a követelményeket, valójában azonban éppen ellenkezőleg, gátjaivá válnak az átláthatóság tényleges érvényesülésének. A háttérben az áll, hogy az adatkezelők célja nem az, hogy az érintettek megértsék a tájékoztatást, hanem az, hogy jogi védelmet biztosítsanak saját maguknak. Megoldásként – a GDPR által is említett – a digitális környezethez jól illeszkedő elem jöhet szóba: az adatvédelmi ikonok használatának előmozdítása (ezzel kapcsolatban a kutatásoknak és a Bizottságnak is vannak tennivalói), ill. bármely olyan elem, ami az

⁴¹¹ GDPR 13–14. cikk

⁴¹² WP260. 16.

⁴¹³ GDPR 13–22. cikk és 34. cikk

⁴¹⁴ WP260. 47.

értelmezhetőséget, a befogadhatóságot segíti, például a táblázatos formák, kiemelések, a tájékoztatók terjedelmének lehetséges zsugorítása.

A digitális omnibusz csomag javaslata az adminisztratív terhek csökkentése érdekében egyszerűbb tájékoztatási kötelezettséget ígér, ha az adatokat az adatkezelő és az érintett közötti „egyértelmű és körülhatárolt kapcsolat keretében gyűjtötték, és alapos okkal feltételezhető, hogy az érintett már rendelkezik” adott információkkal – amennyiben az adatkezelő tevékenysége nem adatintenzív, nem végez automatizált adatkezelést, és nem továbbítja az adatokat harmadik felek részére, valamint az adatkezelés nem magas kockázatú.⁴¹⁵ A javaslat céljával és utóbbi négy feltételével egyetértek, azonban az egyértelmű és körülhatárolt kapcsolatra hivatkozással, valamint azzal, hogy az érintett már rendelkezik az információkkal, nem értek egyet, mert bizonytalan megfogalmazású, és a preambuluma sem teszi egyértelműbbé.

4.2. Az érintett hozzáférési joga

A hozzáférési jog lényege, hogy az érintett a saját személyes adatairól és azok kezeléséről tájékoztatást kapjon, s legfőbb célja az, hogy a saját adatai felett ellenőrzést biztosítson. Hozzájárulhat a tudatos fogyasztói magatartás kialakulásához, hiszen rálátást tesz lehetővé az érintett saját személyes adataira és azok felhasználására. Ezeket a GDPR preambuluma szögezi le: az érintett jogosult arra, hogy „hozzáférjen a rá vonatkozóan gyűjtött adatokhoz, valamint arra, hogy egyszerűen és észszerű időközönként, az adatkezelés jogszerűségének megállapítása és ellenőrzése érdekében gyakorolja e jogát.”⁴¹⁶

A hozzáférési jogot már az adatvédelmi irányelv⁴¹⁷ is tartalmazta, tehát nem új jogintézmény a GDPR-ban, ez utóbbi azonban megerősíti és bővíti is az érintett jogait. Összevetve a két jogszabályt, a hozzáférési jog a következőkkel bővült a GDPR-ban: kiemeli a harmadik országokat és a nemzetközi szervezeteket mint a címzetteket/címzettek kategóriáit, valamint az erre vonatkozó garanciákat; ugyanígy az automatizált döntéshozatal tényével kapcsolatos információkon belül kiemeli a profilalkotást, amellyel kapcsolatban a következményekről való tájékoztatást hangsúlyozza. A korlátozott tárolhatóság elvével összhangban a személyes adatok tárolásának tervezett időtartama vagy ezen időtartam meghatározásának szempontjai szintén a hozzáférési jog körébe tartoznak. Az érintettek

⁴¹⁵ Digitális omnibusz csomag 3. cikk 5. pont, (36) preambulumbekkezdés

⁴¹⁶ GDPR (63) preambulumbekkezdés

⁴¹⁷ Adatvédelmi irányelv 12. cikk

hozzáférési jogának bővülését jelzi az is, hogy az átláthatóság biztosítása és növelése érdekében az érintett kérheti a személyes adatai másolatát.⁴¹⁸

A hozzáférési jognak a kontrolljellege adja erősségét: ellenőrizhető a jogszerűség, növekedik az elszámoltathatóság. Az algoritmusokkal dolgozó adatvezérelt vállalatok adatkezelése azonban – úgy vélem – nehezen vagy alig értelmezhető az átlagfelhasználó számára. A jövő útja egy olyan információs felület, irányítópult (dashboard) lehet, ami interaktív módon, valós időben képes mutatni az adatokat.

4.3. A helyesbítéshez való jog

A helyesbítéshez való jog előfeltétele a hozzáférési jog, hisz ez utóbbi biztosít lehetőséget az érintett számára ahhoz, hogy személyes adatait ellenőrizze, majd az esetlegesen pontatlan vagy hiányos adatait helyesbíttesse, kiegészíttesse. A helyesbítéshez való jog az adatvédelmi irányelvhez képest tartalmában nem változott a GDPR-ban, csak pontosítása történt: az érintett jogosult arra, hogy a rá vonatkozó pontatlan adatok helyesbítését kérje, amit az adatkezelő indokolatlan késedelem nélkül köteles megtenni; valamint a hiányos személyes adatok kiegészítését kérheti az érintett, ennek mércéje az adatkezelés célja. Az adatkezelőnek értesítenie kell minden olyan további adatkezelőt, címzettet, akivel, amellyel a helyesbítéssel érintett adatot közölték.⁴¹⁹

Mivel a személyes adatok kezelésére vonatkozó elvek egyike a pontosság, ezért minden észszerű intézkedést meg kell tenni annak érdekében, hogy az adatkezelés céljai szempontjából pontatlan személyes adatokat haladéktalanul helyesbítsék.⁴²⁰ Az adatkezelő abban az esetben köteles helyesbíteni a személyes adatot, ha a kérelmező bizonyítékot tud szolgáltatni kérése alátámasztására. A tényadatok, például a cím vagy a születési dátum helyesbítése nem okozhat problémát, mert azok könnyen bizonyíthatók, de előfordulnak olyan esetek is, amikor nehezebb a bizonyítás. Ezt mutatja az EUB-nek a Deldits-ügyben előzetes döntéshozatali kérelemre született ítélete.⁴²¹ VP nőként született, de férfi nemi identitással rendelkezik, aki helyesbítési kérelmet terjesztett elő a menekültügyi hatóságnál arra vonatkozóan, hogy a nemére vonatkozó bejegyzést férfire javítsák. A hatóság azzal az indoklással utasította el a kérelmet, hogy a VP által csatolt egészségügyi dokumentáció nem elegendő, nemváltoztató műtétről is igazolás

⁴¹⁸ GDPR 15. cikk (1)–(2) bekezdés

⁴¹⁹ GDPR 19. cikk

⁴²⁰ GDPR 5. cikk (1) bekezdés d) pont

⁴²¹ ECLI:EU:C:2025:172. A Bíróság ítélete (első tanács) a C-247/23. sz. Deldits-ügyben (helyesbítéshez való jog a nemi identitásra vonatkozóan), 2025. március 13. (a továbbiakban a lábjegyzetekben: EUB-ítélet C-247/23. sz. ügy)

szükséges. Az ügyben a Fővárosi Törvényszék fordult az EUB-hoz, amely nemcsak azt erősítette meg, hogy a pontatlan személyes adatokat köteles az adatkezelő helyesbíteni, de azt is, hogy a joggyakorló kötelezhető „olyan releváns és elegendő” bizonyíték szolgáltatására, amely az „adatok pontatlanságának megállapításához észszerűen megkövetelhető,” ugyanakkor nem követelhető meg – sem az EJEB ítélkezési gyakorlata, sem a Charta 3. és 7. cikke alapján – nemváltó műtét, így erre vonatkozó igazolás sem kérhető.⁴²²

A helyesbítéshez való jog különösen hasznos lehet az automatizált döntéshozatallal és profilalkotással kapcsolatos személyesadat-kezelés során, amikor csoportokba, kategóriákba sorolják az érintetteket. Előfordulhat, hogy pontatlan, lényegtelen adatokat használtak, esetleg kiragadták az adatokat az összefüggésből, ilyenkor a személyes adatokhoz kiegészítések, pontosítások tehetők, mind a bemeneti (a profil létrehozásához használt), mind a kimeneti (maga a profil vagy a személyhez rendelt mutató, érték) adatokra vonatkozóan.⁴²³ Az adatkezelők fontolóra vehetik online preferenciakezelési eszközök (pl. adatvédelmi jelzőrendszer) bevezetését. Ez lehetőséget ad az érintetteknek arra, hogy közvetlenül maguk kezeljék a beállítások megváltoztatását, a személyes adataik frissítését vagy a profiljuk áttekintését, szerkesztését az esetleges pontatlanságok helyesbítése érdekében.⁴²⁴ A gyakorlat azonban azt mutatja, hogy a többnyire kikövetkeztetett adatokat tartalmazó profil helyesbítése nem mindig működik gördülékenyen. A profilalkotással keletkezett, jövőbeli magatartásra vonatkozó predikciók nem mérhetők, objektíven nem ellenőrizhető az adat pontossága, ezért az adatkezelő elutasíthatja a helyesbítési kérelmet.⁴²⁵ Álláspontom szerint ezeket pusztán a szóban forgó jog gyakorlásával már nehéz kezelni, ehhez az adatkezelő folyamatos ellenőrzésére és az érintettek kollektív fellépésére is szükség lehet. Az egyéni jogérvényesítés több érintetti jog együttes alkalmazását is megkívánja: az adatkezelés korlátozásához való jogot, a tiltakozás jogát, az automatizált döntéshozatal elleni védelmet.

4.4. A törléshez való jog (elfeledtetéshez való jog)

Az adatvédelmi irányelv már nevesítette a törléshez való jogot (data erasure).⁴²⁶ A GDPR 17. cikke nemcsak megerősíti ezt a jogot, de kiszélesíti a tartalmát, és „elfeledtetéshez való jog” (right to be forgotten) néven illeszti a rendeletbe. Ez alapján az érintett jogosult arra,

⁴²² EUB-ítélet C-247/23. sz. ügy 51. pont

⁴²³ WP251. 18–19.

⁴²⁴ WP251. 34.

⁴²⁵ Andreas HÄUSELMANN – Bart CUSTERS: *The Right to Rectification and Inferred Personal Data*. European Journal of Law and Technology, 2024/3. 23. <https://ejlt.org/index.php/ejlt/article/view/1004/1097> (letöltés: 2025. 09. 08.)

⁴²⁶ Adatvédelmi irányelv 12. cikk

hogy bármikor kérje, és hogy kérésére az adatkezelő indokolatlan késedelem nélkül törölje a rá vonatkozó személyes adatokat; az adatkezelő pedig köteles ezt megtenni, ha a következő indokok valamelyike fennáll: a személyes adatokra már nincs szükség az eredeti célból; az érintett visszavonja hozzájárulását, és az adatkezelésnek nincs más jogalapja; az érintett tiltakozik az adatkezelés ellen, és nincs elsőbbséget élvező jogszerű ok az adatkezelésre; uniós vagy tagállami jogban előírt jogi kötelezettség teljesítéséhez törölni kell stb.⁴²⁷

A harmadik félnek továbbított adatok esetében az adatvédelmi irányelv alapján az érintettnek külön kérnie kellett az adatkezelőt, hogy intézkedjen a törlésről; a GDPR ezt az adatkezelők feladatává teszi. Ennek eredményeként az érintett adat többé nem elérhető és nem visszaállítható az interneten, amivel megvalósul a GDPR új jogintézménye: az elfeledtetéshez való jog. A folyamat megvalósíthatóságát azonban kétséggé teszi magának a rendelkezésnek a megfogalmazása: egyrészt csupán a harmadik felek arra vonatkozó tájékoztatását írja elő, hogy az érintett kérte a törlést; másrészt az adatkezelőnek csupán „észszerűen elvárható” lépéseket kell tenni; és harmadrészt ezt is csak a megvalósítási költségek figyelembevétel.⁴²⁸ A gyakorlatban ez a rendelkezés nem garantálja a teljes törlést.

Az elfeledtetéshez való jog beillesztése a GDPR-ba egy konkrét jogeset⁴²⁹ alapján történt: A spanyol adatvédelmi hatósághoz panasz érkezett egyrészt egy napilap kiadója ellen, mert adótartozással összefüggő ingatlanárveréssel kapcsolatban konkrét név szerepelt, másrészt a név birtokosa azt is kérte, hogy ezek az adatok ne jelenjenek meg a Google keresési találatai között, és ne kapcsolódjanak a kiadó linkjeihez. Az adatvédelmi szerv a kiadó ellen nem adott helyt a panasznak, mert – bár főszabályként az adatvédelmi jogok megelőzik a tájékoztatáshoz való jogot – jelen esetben az információs szabadsághoz és a véleménynyilvánításhoz fűződő jogot ítélte erősebbnek; a Google vonatkozásában azonban helyt adott a panasznak, azzal az indokkal, hogy az információs társadalom közvetítője, s ezáltal adatkezelő. A Google a spanyol legfelsőbb bírósághoz nyújtott be keresetet a határozat ellen, amely előzetes döntéshozatali eljárás keretében két kérdéssel fordult az EUB-hez: milyen kötelezettségei vannak a keresőmotorok működtetőinek azon érintett személyek adatainak védelmében, akik nem szeretnék, hogy hozzáférhetővé tegyék az internetfelhasználók számára harmadik fél honlapján megjelenő adataikat; ill. a Google adatkezelőnek minősül-e. Az EUB szerint a keresőmotorok tevékenysége – mivel a találati listák megjelenítésével a személyes adatokat terjeszti – alkalmas arra, hogy nagymértékben érintse a magánélethez fűződő

⁴²⁷ GDPR 17. cikk (1) bekezdés

⁴²⁸ GDPR 17. cikk (2) bekezdés

⁴²⁹ EUB-ítélet C-131/12. sz. ügy

személyes jogot, és a keresőmotor működtetője adatkezelőként felelős azok védelméért. Itt szerepelt először nevesítve „az internet »felejtéséhez« való jog,”⁴³⁰ vagyis az elfeledtetéshez való jog, kiegészítve a törléshez való jogot. Az, hogy a spanyol napilapban nem változtatták meg az archivált adatokat, arra is rámutat, hogy az elfeledtetéshez való jog nem superjog, nem írja felül az alapvető jogokat.⁴³¹ Ha az adatkezelő más joggal is rendelkezik az adatok kezelésére, akkor az érintett személy törekvése ellenére is folytathatja a tevékenységet.

A GDPR pontosan meghatározza az elfeledtetés korlátait. Nem alkalmazandó, amennyiben az adatkezelés szükséges: a véleménynyilvánítás szabadságához és a tájékozódáshoz való jog gyakorlása céljából; a személyes adatok kezelését előíró, az adatkezelőre alkalmazandó uniós vagy tagállami jog szerinti kötelezettség teljesítése céljából; a népegészségügy területét érintő közérdek alapján; közérdekű archiválás céljából, tudományos és történelmi kutatási vagy statisztikai célból, amennyiben a törléshez való jog valószínűsíthetően lehetetlenné tenné vagy komolyan veszélyeztetné ezt az adatkezelést; vagy jogi igények előterjesztéséhez, érvényesítéséhez, ill. védelméhez.⁴³² Ha a felsoroltak valamelyike fennáll, akkor az adatkezelőnek kell bizonyítania, hogy az adatra még szükség van, ezért nem törölhető, vagyis megfordul a bizonyítási teher. Szintén az érintettek érdekeit szolgálja az, hogy mivel a GDPR hatálya minden adatkezelőre kiterjed, amely uniós polgárok adatait kezeli, ezért a törléshez, az elfeledtetéshez való jog is vonatkozik az Európán kívüli adatkezelőkre, keresőmotorok üzemeltetőire is.

A végleges törlés lehetősége értékes előrelépés, ugyanakkor – a harmadik felek részére továbbított személyes adatok tekintetében – csak korlátozottan biztosít az érintettek számára kontrollt, noha a cél valójában az elfeledtetés. Példaként említhető a törlés lehetetlensége a természetes személy ellenőrzése alól kikerült biometrikus azonosító esetén, ha az megjelent az interneten.⁴³³ A törlés jelentőségét abban látom, hogy mivel az adatokból létrejött összkép meghatározza a piaci (pl. hitelhez, platformhoz) hozzáférés lehetőségeit, az elfeledtetéshez való joggal az egyén aktualizálhatja és ezáltal korrigálhatja ezt az összképet, a profilt.

4.5. Az adatkezelés korlátozásához való jog

Az adatkezelés korlátozásához való jog nem szerepel az adatvédelmi irányelvben, mégsem teljesen új jog. Az irányelv az adathozzáféréshez való jogon belül biztosította azt, hogy

⁴³⁰ EUB-ítélet C-131/12. sz. ügy 91. pont

⁴³¹ KAPPEL Gergely – SIMON Soma: *Az elfeledtetéshez való jog – Európára korlátozva?* Arsboni 2020. február 17. <https://arsboni.hu/az-elfeledteteshez-valo-jog-europ/> (letöltés: 2021. 11. 22.)

⁴³² GDPR 17. cikk (3) bekezdés

⁴³³ G. KARÁCSONY (2022) i. m. 309.

az érintett kérje az olyan adatok zárolását (vagy helyesbítését, törlését), amelyek feldolgozása nem felel meg az említett irányelv rendelkezéseinek, különösen az ilyen adatok hiányos vagy hibás volta miatt.⁴³⁴ A GDPR szétbontotta és pontosította e jogot.

Az adatkezelés korlátozásához való jog az érintett joga, az ő kérésére korlátozza az adatkezelő az adatkezelést a következő feltételek valamelyikének teljesülése esetén: az érintett vitatja a személyes adatok pontosságát, ez esetben a korlátozás arra az időtartamra vonatkozik, amely lehetővé teszi, hogy az adatkezelő ellenőrizze a személyes adatok pontosságát; az adatkezelés jogellenes, és az érintett ellenzi az adatok törlését, és ehelyett kéri azok felhasználásának korlátozását; az adatkezelőnek már nincs szüksége a személyes adatokra adatkezelés céljából, de az érintett igényli azokat jogi igények előterjesztéséhez, érvényesítéséhez vagy védelméhez; vagy az érintett tiltakozott az adatkezelés ellen; ez esetben a korlátozás arra az időtartamra vonatkozik, amíg megállapításra nem kerül, hogy az adatkezelő jogos indokai elsőbbséget élveznek-e az érintett jogos indokaival szemben.⁴³⁵ A felsorolt esetekben csupán a személyes adatok tárolása történhet, a felhasználásuk nem. A tárolás időtartamát vagy az adatkezelőre vonatkozó kötelezettségek szabják meg, vagy az érintett és a hozzá kapcsolódó jogi és egyéb igények.

Az adatkezelés korlátozásához való jog értéke: a jogviták rendezése során az érintett érdekét, a méltányosságot tartja szem előtt; ugyanakkor, mivel szorosan kapcsolódik más jogokhoz, önállóan ritkán alkalmazzák.⁴³⁶

4.6. Az adathordozhatósághoz való jog

Az érintettek jogai közé tartozik az adathordozhatósághoz való jog (data portability), amelynek nincs előzménye az adatvédelmi irányelvben, új jogintézményként jelent meg a GDPR-ban. Hátterében az áll, hogy a jogalkotó figyelembe vette a dolgok internete (Internet of Things; a továbbiakban: IoT) körébe tartozó eszközök, okosotthon-megoldások vagy akár az elektronikus levelezés elterjedtségét, és ehhez igazította az adathordozhatósághoz való jog célját: az érintettek tudatos magatartásra ösztönzése, ezzel együtt nagyobb rendelkezés biztosítása számukra a személyes adataik felett.⁴³⁷

⁴³⁴ Adatvédelmi irányelv (12) cikk b) pont

⁴³⁵ GDPR 18. cikk (1) bekezdés

⁴³⁶ Gloria González FUSTER: *Article 18 Right to restriction of processing*. In: Christopher KUNER et. al: *The EU General Data Protection Regulation (GDPR): A Commentary*. 2020. 485–491. <https://academic.oup.com/oxford-law-pro/book/41324/chapter-abstract/352298156?redirectedFrom=fulltext&login=false> (letöltés: 2024. 01. 20.)

⁴³⁷ WP242. A 29. cikk szerinti munkacsoport: Iránymutatás az adatok hordozhatóságáról. 3.

A GDPR megvilágítja az adathordozhatósághoz való jog tartalmát: „Az érintett jogosult arra, hogy a rá vonatkozó, általa egy adatkezelő rendelkezésére bocsátott személyes adatokat [...] géppel olvasható formátumban megkapja,” és hogy ezeket egy másik adatkezelőnek továbbítsa.⁴³⁸ A definíció két feltételt határoz meg ahhoz, hogy a személyes adat az adathordozhatóság hatálya alá tartozzon: az érintettre vonatkozó személyes adatnak kell lennie, és egyúttal olyan adatnak, amelyet az érintett bocsátott az adatkezelő rendelkezésére. Előbbivel kapcsolatban fölmerülhet a kérdés, hogy az álnevesített adatra kiterjed-e az adathordozhatóság lehetősége. Mivel személyes adatnak minősül, ezért ha az érintett megadja a megfelelő azonosítót, akkor igennel válaszolhatunk a kérdésre, és az adathordozhatósági kérelem hatálya alá tartozhat.⁴³⁹ A másik problémát az olyan adathordozhatósági kérelmek okozhatják, amelyek megválaszolásában több érintett adatai szerepelnek, például a telefonbeszélgetések listái harmadik személyre vonatkozó személyes adatokat is tartalmazhatnak, ilyenkor – mivel az érintettre is vonatkoznak – ezeket is rendelkezésre kell bocsátani.⁴⁴⁰ Arra az adathordozhatósági feltételre vonatkozóan, hogy a személyes adatot az érintettnek kell az adatkezelő rendelkezésére bocsátania, sok példa hozható, például a formanyomtatványokon megadott e-mail-fiók adatai, sőt a 29. cikk szerinti munkacsoport szerint ki kell terjednie azokra a személyes adatokra is, amelyeket a felhasználói tevékenységgel kapcsolatban figyeltek meg, például a keresési tevékenységek adataira, ha azokat nem az adatkezelő hozta létre, vagyis ha nem elemezte a megfigyelt adatokat.⁴⁴¹ Annak érdekében, hogy egyértelműen eldönthető legyen, hogy mely adatkategóriákra terjed ki az adathordozhatóság, szét kell választani eredetük alapján az érintett által rendelkezésre bocsátott személyes adatokat: tudatosan és aktívan rendelkezésre bocsátott adatok (pl. az e-mail-cím), ill. az érintett által a szolgáltatás vagy a készülék használatával rendelkezésre bocsátott, megfigyelt adatok (pl. a keresési tevékenységek adatai, valamint a GPS-adatok).⁴⁴² A GDPR rendelkezéseiből idevonatkozóan egy harmadik feltételt is említeni kell: az adathordozhatósághoz való jog nem érintheti hátrányosan mások jogait és szabadságait. E feltétel kiterjed a más érintettekre vonatkozó személyes adatokra,⁴⁴³ ideértve a szellemi tulajdon és az üzleti titok hatálya alá tartozó adatokat is.

Az adathordozhatósághoz való jog gyakorlása során az érintett arra is jogosult, hogy – ha technikailag megvalósítható – kérje a személyes adatok adatkezelők közötti közvetlen

⁴³⁸ GDPR 20. cikk (1) bekezdés

⁴³⁹ GDPR 11. cikk (2) bekezdés; WP242. 10.

⁴⁴⁰ WP242. 10–11.

⁴⁴¹ WP242. 11.

⁴⁴² WP242. 11.

⁴⁴³ GDPR 20. cikk (4) bekezdés

továbbítását.⁴⁴⁴ E rendelkezés elősegíti a személyes adatok szabad áramlását az EU-ban, élénkíti a versenyt az adatkezelők között, valamint megkönnyíti a különböző szolgáltatók közötti váltást, ezért előmozdítja új szolgáltatások kidolgozását a digitális egységes piaci stratégiával összefüggésben.⁴⁴⁵ A GDPR alapján az adathordozhatóság következő elemei rajzolódnak ki: a személyes adatok megszerzésének joga, ezek adatkezelők közötti továbbításának joga, az adatkezelői jogállás, valamint az adathordozhatóság és az érintettek egyéb jogainak összefüggése.⁴⁴⁶ Kiemelve az adatkezelők közötti továbbítás jogát, ez tulajdonképpen az átjárhatóságot, az interoperabilitást jelenti. A GDPR nem teremt olyan kötelezettséget az adatkezelők számára, hogy egymással műszakilag kompatibilis adatkezelő rendszereket vezessenek be,⁴⁴⁷ de ösztönzi őket arra, hogy az adathordozhatóságot lehetővé tevő interoperábilis formátumokat fejlesszenek ki,⁴⁴⁸ különös tekintettel az ágazati felek és a szakmai szervezetek vonatkozásában. Ezzel párhuzamosan a GDPR megtiltja az adatkezelőknek, hogy akadályozzák az adattovábbítást.⁴⁴⁹ Az interoperabilitás hiánya nem segíti az adathordozhatósághoz való jog érvényesíthetőségét, inkább gátolja azt, és tágabban a tudatos fogyasztói magatartás kialakulását is.

Az adathozzáférést és -hordozhatóságot a legértékesebb érintetti jognak tartom, amelyben harmóniába olvad a GDPR címében is hangsúlyozott kettős cél: a benne foglalt kontroll az érintettek védelmét szolgálja; egyúttal lehetőséget teremt az adatok szabad áramlásának biztosítására. Konkrét jelentősége felmérhetetlen a ma már igen elterjedt IoT-termékek által generált adatok használatával kapcsolatban. Amikor ezeket a fogyasztó megkapja, lehetősége van arra, hogy vagy maga továbbítsa például valamely szakszerviz részére, vagy kérje az adatkezelők közötti közvetlen továbbítást. Utóbbi azonban a GDPR interoperabilitásra vonatkozó kettős megközelítése miatt gyakorlatilag lehetetlen. Ebben látom az okát annak, hogy ez a jogintézmény nem vált népszerűvé, holott az említett termékek egyre népszerűbbek, és a piaci folyamatokra vonatkozóan is potenciált hordoz.

4.7. A tiltakozáshoz való jog

A GDPR alapján az érintett jogosult arra, hogy a személyesadat-kezelésre vonatkozó hozzájárulását visszavonja, hogy adott feltételek esetén az adatkezelő törölje az adatait, ill. hogy

⁴⁴⁴ GDPR 20. cikk (2) bekezdés

⁴⁴⁵ WP242. 3.

⁴⁴⁶ GDPR 20. cikk (1)–(2) bekezdés

⁴⁴⁷ WP242. 5.

⁴⁴⁸ GDPR (68) preambulumbekkezdés

⁴⁴⁹ GDPR 20. cikk (1) bekezdés

tiltakozzon a már elkezdett adatkezelés ellen. A tiltakozáshoz való jog és a törléshez való jog közötti lényeges különbség az, hogy előbbi az adott személyes adat további, előre meghatározott célú kezelésének megszüntetésére irányul, míg utóbbi esetben minden célból megszűnik az adatkezelés, az adatkezelő egyáltalán nem tárolhatja tovább az adatot. A személyes adatok kezelése elleni tiltakozási jogot csak néhány esetben biztosítja a GDPR: a közvetlen üzletszerzés érdekében történő adatkezelés, valamint a közérdekű adatkezelésen és a jogos érdeken alapuló adatkezelés esetén; más célú adatkezelésre nem biztosítja.

A mindennapi életben a magánszemélyek gyakran iratkoznak fel hírlevélre, regisztrálnak adatkezelő nyilvántartásokban, következésképpen reklámokat, hírleveleket kapnak; ill. az online vásárlásaik, sőt a kereséseik alapján gyakran alkotnak profilt a cégek, és ezek alapján hirdetésekkel bombázzák őket. Ezeknek a közös jellemzője a közvetlen üzletszerzési cél. A közvetlen üzletszerzés érdekében történő személyesadat-kezelés – ideértve a profilozást is – ellen az érintett bármikor és ingyenesen tiltakozhat. Ilyen esetekben az adatkezelőnek nem kell mérlegelni; a személyes adatok a továbbiakban e célból nem kezelhetők, ami az adatok törlésére vonatkozó kötelezettséget is magával vonja.⁴⁵⁰ A közvetlen üzletszerzésre irányuló adatkezelés elleni tiltakozás tehát abszolút, feltétlen jognak tekintendő.⁴⁵¹ A tiltakozáshoz való jognak ez a sajátossága csak a GDPR-ra jellemző, az adatvédelmi irányelv nem tartalmazta.

A jogalkotó akkor is biztosítja a személyes adatok kezelése (ideértve a profilalkotást is) elleni tiltakozási jogot, ha a személyes adatok jogszerűen kezelhetők, mert az adatkezelésre közérdekből vagy közhatalmi jogosítvány gyakorlása keretében végzett feladat végrehajtásához, ill. jogos érdek alapján van szükség.⁴⁵² Tiltakozás esetén az adatkezelő a személyes adatokat nem kezelheti tovább,⁴⁵³ kivéve, ha bizonyítja, hogy az adatkezelést olyan kényszerítő erejű jogos okok indokolják, amelyek elsőbbséget élveznek az érintett érdekeivel, jogaival és szabadságaival szemben, vagy amelyek jogi igények előterjesztéséhez, érvényesítéséhez vagy védelméhez kapcsolódnak.⁴⁵⁴ Arra vonatkozóan, hogy mit jelent a „kényszerítő erejű” kifejezés a profilalkotás esetén, a 29. cikk szerinti munkacsoport ad magyarázatot: a profilalkotás hasznos valamely tágabb közösség számára, és nem csak az adatkezelő üzleti érdekei szempontjából. Példaként említhető az az eset, ha a profilalkotás a fertőző betegségek terjedését jelzi előre.⁴⁵⁵ A kényszerítő erejű jogos ok vizsgálatára sincs

⁴⁵⁰ GDPR (70) preambulumbekkezdés és 21. cikk (2)–(3) bekezdés

⁴⁵¹ DÉNESNÉ ORCSIK Judit: *2018-tól jön a modernebb, de szigorúbb adatvédelem*. Ügyvédvilág 2016/4. 14.

⁴⁵² GDPR (69) preambulumbekkezdés

⁴⁵³ GDPR 18. cikk (1) bekezdés d) pont

⁴⁵⁴ GDPR 21. cikk (1) bekezdés

⁴⁵⁵ WP251. 20.

szükség azonban azokban az esetekben, amikor a tiltakozást követő törlés nem alkalmazható, például ha az adatkezelés a véleménynyilvánítás szabadságához és a tájékozódáshoz való jog gyakorlásához szükséges.⁴⁵⁶ Ezt mutatja az a Kúria elé került ügy, amelynek alperese „Az 50 leggazdagabb magyar” című kiadvány összeállítója, egyben adatkezelője, és felperese az az üzletember, aki a magánszférához és a személyes adatok védelméhez való jogra hivatkozva tiltakozott az adatkezelés ellen. Központi kérdésként az fogalmazódott meg, hogy az üzletember tiltakozása felülírja-e az adatkezelő jogos érdekét.⁴⁵⁷ A Kúria azt állapította meg, hogy mivel a véleménynyilvánítás szabadsága céljából – jogos érdek alapján – az adatok kezelése szükséges volt, ehhez már nem szükséges a kényszerítő erejű jogos ok vizsgálata, ezért a tiltakozás „nem vezethet a törlés jogkövetkezményének alkalmazásához.”⁴⁵⁸ A jogos érdek tehát bizonyos esetekben, így a véleménynyilvánítás szabadsága szempontjából, egyben kényszerítő erejű ok is, és az érintett tiltakozása esetén sem törölhetők a személyes adatok. Az önrendelkezéshez fűződő alkotmányos alapjog és a véleménynyilvánításhoz fűződő alkotmányos alapjog, a sajtószabadság közötti normaütközés összevethető érdekmérlegelési tesztel, amelynek eredménye jelen ügyben az a megállapítás volt, hogy a személyes adatok védelméhez való jog nem abszolút jog, korlátozása az alapjogi teszt feltételei szerint megengedett, de kizárólag a szükséges és arányos mértékű beavatkozás szintjére szorítva.⁴⁵⁹

A tiltakozás jogát az érintetteket erőteljesen védő perspektívája miatt az egyik legértékesebb érintetti jognak tartom. Míg a gyakorlatban a helyesbítéshez való jog nehézkes, a törléshez való jog csak korlátozottan működőképes, addig a tiltakozáshoz való jog – a közvetlen üzletszerzésre irányuló adatkezelés ellen – abszolút. Ezzel magyarázható az is, hogy az EUB esetjogában nem szerepel a tiltakozás értelmezésére vonatkozó ügy, a direkt marketing fogalmának tág értelmezése mellett azonban többször állást foglalt,⁴⁶⁰ ami erősíti a tiltakozáshoz való jog gyakorlati jelentőségét. Más adatkezelési célnál a vonatkozó rendelkezés megfogalmazása („kényszerítő erejű jogos okok”) bizonytalan értelmezéshez is vezethet.

4.8. Automatizált döntéshozatal egyedi ügyekben, beleértve a profilalkotást is

A már bemutatott rendelkezések esetében a cikkek címei rámutatnak arra, hogy az érintettre vonatkozó jogot fogalmazzák meg, az Automatizált döntéshozatal egyedi ügyekben,

⁴⁵⁶ GDPR 17. cikk (3) bekezdés a) pont

⁴⁵⁷ BH 2025.1.13. A GDPR 6. cikk (1) bekezdés f) pontja alapján három feltétel együttes teljesülése szükséges a természetes személyek személyes adatainak jogszerű kezeléséhez: 1. az adatkezelő [...]

⁴⁵⁸ BH 2025.1.13. (76) bekezdés

⁴⁵⁹ BH 2025.1.13. (50) bekezdés

⁴⁶⁰ ECLI:EU:C:2025:871. A Bíróság ítélete (első tanács) a C-654/23. sz. ügyben, 2025. november 13.

beleértve a profilalkotást cím azonban nem tartalmazza a jog szót. Ennek magyarázata az, hogy itt főszabályként általános tilalom vonatkozik az adatkezelésre, az érintettnek nincs érvényesíthető joga, csak passzív joga keletkezik.⁴⁶¹ A háttérben az információs önrendelkezési jog helyett az emberi méltóság tiszteletben tartása áll, amely „az emberi személyt léténél fogva többnek tartja múltbéli információkból összeállítható profilnál.”⁴⁶²

A GDPR-ban az automatizált adatkezelés és az automatizált döntéshozatal fogalmakkal találkozunk. Az automatizált adatkezelés azt jelenti, hogy az adatok gyűjtése, elemzése stb. számítógépes rendszerek és algoritmusok segítségével történik. Ennek egy speciális típusa az automatizált döntéshozatal, melynek során a rendszer nemcsak feldolgozza az adatokat, hanem azok alapján döntést is hoz. Az automatizált döntéshozatal fogalmát a GDPR nem határozza meg, definíciója a 29. cikk szerinti munkacsoport iránymutatásában található: „az a képesség, hogy technológiai eszközök segítségével, azaz emberi beavatkozás nélkül hoznak döntéseket,” amelyek bármilyen személyes adaton alapulhatnak. Ezek az adatok lehetnek akár az érintett által megadott, akár természetes személyekről megfigyelt (pl. alkalmazás révén gyűjtött helymeghatározási adatok), akár származtatott vagy kikövetkeztetett adatok (pl. hitelminősítési pontszám).⁴⁶³ A European Law Institute⁴⁶⁴ fogalommeghatározása a teljes folyamatot hangsúlyozza: Az automatizált döntéshozatal olyan folyamat, amely a kapott vagy gyűjtött bemeneti adatok alapján, előre meghatározott célok mentén, sokféle formában (értékelések, döntések, előrejelzések stb.) képes kimeneteket generálni.⁴⁶⁵ Minden automatizált döntéshozatal algoritmikus rendszeren alapul,⁴⁶⁶ amely adott feladat elvégzéséhez vagy egy probléma megoldásához vezető lépések sorát jelenti.

A GDPR-ban az automatizált adatkezelés és az automatizált döntéshozatal fogalmak mellett megjelenik a profilalkotás fogalom is, a definíciójával együtt,⁴⁶⁷ ezt építi tovább a munkacsoport meghatározása: egy természetes személyről való információgyűjtést és a jellemzői vagy a viselkedési mintái értékelését jelenti abból a célból, hogy valamely

⁴⁶¹ WP251. 21.

⁴⁶² TÖRÖK Bernát: Az „empíria-feletti” ember. Jogtudományi Közlöny 2025/12. 534. <https://doi.org/10.59851/jk.80.12.3> (letöltés: 2026. 01. 02.)

⁴⁶³ WP251. 8.

⁴⁶⁴ Független non-profit szervezet, amelyet azzal a céllal hoztak létre, hogy kutatásokat kezdeményezzen, végezzen és segítsen, ajánlásokat fogalmazzon meg, valamint gyakorlati útmutatást nyújtson az európai jogfejlesztés területén.

⁴⁶⁵ ELI: *Guiding Principles for Automated Decision-Making in the EU*. ELI Innovation Paper. 8. https://www.europeanlawinstitute.eu/fileadmin/user_upload/p_eli/Publications/ELI_Innovation_Paper_on_Guiding_Principles_for_ADM_in_the_EU.pdf (letöltés: 2025. 01. 03.)

⁴⁶⁶ Ugyanakkor nem minden algoritmikus rendszer hoz automatizált döntést. Egy algoritmikus rendszer pl. szűrhet vagy elemezhet anélkül adatokat, hogy önálló döntést hozna. Az automatikus döntéshozatal esetében azonban a rendszer célja éppen a döntéshozás.

⁴⁶⁷ GDPR 4. cikk 4. pont

kategóriába vagy csoportba besorolja őt, különösen, hogy elemezze és/vagy előrejelzéseket állapítson meg például egy feladat végrehajtására való képességéről, érdeklődési köréről vagy várható magatartásáról.⁴⁶⁸ Az automatizált döntéshozatal és a profilalkotás nem feltétlenül egymást feltételező folyamatok, automatizált döntést lehet hozni profilalkotással vagy anélkül; és profilalkotás is történhet automatizált döntéshozatallal és anélkül is, ugyanakkor az automatizált döntéshozatal átalakulhat profilalkotássá. Például a sebességmérő kamerái által rögzített bizonyítékok alapján a gyorsrajtási bírság kiszabása automatikus döntéshozatal, de ha a bírság összegét más, a természetes személy vezetési szokásait jellemző tényezők (pl. ismétlődő szabálysértés) is meghatározzák, akkor már profilalkotáson alapul a döntés.⁴⁶⁹

A GDPR 22. cikke foglalkozik az automatizált döntéshozatallal, amely címében tágabb kört jelez, mint a cikk rendelkezései, amelyek a kizárólag automatizált döntésekre vonatkoznak. Ez azt jelenti, hogy az automatizálásnak többféle típusa létezik, és az említett rendelkezések az emberi kontroll nélküli, nagy kockázatot hordozó automatizált döntéseket szabályozzák. Ezek három jellemzője: „kizárólag automatizált adatkezelésen” alapulnak; döntéshozatal történik (igen vagy nem, javasol vagy nem); „joghatással” vagy jelentős hatással járnak (az érintett számára következményei vannak: felveszik adott munkahelyre vagy nem).⁴⁷⁰ A kizárólag automatizált döntéshozatalnak, beleértve a profilalkotást is, meg kell felelni az adatvédelmi elveknek, és az adatkezeléshez megfelelő jogalappal kell az adatkezelőknek rendelkezniük.

„Az érintett jogosult arra, hogy ne terjedjen ki rá az olyan, kizárólag automatizált adatkezelésen – ideértve a profilalkotást is – alapuló döntés hatálya, amely rá nézve joghatással járna vagy őt hasonlóképpen jelentős mértékben érintené.”⁴⁷¹ Az érintett oldaláról ez azt jelenti, hogy aktívan semmit nem kell tennie; a másik oldalon pedig tilalmat fogalmaz meg a kizárólag automatizált adatkezelésen alapuló döntéshozatal tekintetében, ha annak súlyos következménye lehet. Ezzel a GDPR a természetes személyeket automatikusan védi az ilyen adatkezelések hatásaitól.⁴⁷² Ezt támasztja alá az is, hogy e főszabályhoz három kivételt rendel a jogalkotó: megengedhető a kizárólag automatizált adatkezelésen alapuló döntéshozatal: ha szerződésen vagy azt megelőző adatkezelésen alapul, például egy magyarországi állandó lakcímmel rendelkezők számára hirdetett pályázattal kapcsolatban automatizált eszközzel szűrhetik ki azokat, akiknek nincs ilyen lakcímük; ha uniós vagy tagállami jogon alapul: például az adócsalás nyomon követése és megelőzése esetén; vagy ha az érintett kifejezett hozzájárulásán

⁴⁶⁸ WP251. 8.

⁴⁶⁹ WP251. 8.

⁴⁷⁰ GDPR 22. cikk (1) bekezdés

⁴⁷¹ GDPR 22. cikk (1) bekezdés

⁴⁷² WP251. 21.

alapul: ez esetben az érintettnek írásbeli nyilatkozatot kell tennie.⁴⁷³ Ezekben az esetekben az adatkezelő köteles megfelelő intézkedéseket tenni annak érdekében, hogy az érintett az adatkezelőtől emberi beavatkozást kérjen, és hogy kifogást nyújtson be a döntéssel szemben.⁴⁷⁴

Az EUB a Schufa-ügyben az automatizált egyedi döntéshozatalt vizsgálta. OQ hitelkérelmét a bank elutasította a Schufa ügynökség által a fizetőképességére megállapított kedvezőtlen valószínűségi érték alapján. Az ügyben egy német bíróság arra vonatkozóan kért előzetes döntéshozatalt, hogy a valószínűségi érték joghatással járó vagy jelentős mértékű döntésnek minősül-e, ha a bankok ezt automatikusan használják a hitelnyújtási gyakorlatukban. Az EUB megállapította, hogy a valószínűségi érték automatizált megállapítása automatizált egyedi döntésnek minősül, amennyiben döntően ettől az értéktől függ, hogy a bank, akivel ezt az értéket közlik, nyújt-e hitelt, vagy sem.⁴⁷⁵ A Schufa-ügy rámutat arra, hogy a valószínűségi érték nem önmagában mint adat, hanem a hatását, a döntést tekintve fontos, ezért a helyesbítés vagy a törlés nem jelent elegendő védekezést ellene, mindenképpen szükséges az emberi felülvizsgálat.⁴⁷⁶ Az EUB-ítélet azt is megállapította, hogy a 22. cikk rendelkezései nemcsak a hitelező bankra vonatkoznak, hanem az ügynökségre is, következésképp más szervezetre is, amelyek kritikus döntéshozatalhoz támogatást nyújtanak.⁴⁷⁷

A kizárólag automatikus adatkezelésen alapuló döntéshozatal és a profilalkotás a személyes adatok különleges kategóriái vonatkozásában csak két feltétel együttes érvényesülése esetén megengedett: ha szerződésen, uniós vagy tagállami jogon, vagy érintetti hozzájárulásán alapul; és az adatkezelés jelentős közérdek miatt szükséges, uniós jog vagy tagállami jog alapján, amely arányos az elérni kívánt céllal, tiszteletben tartja a személyes adatok védelméhez való jog lényeges tartalmát, és az érintett alapvető jogainak és érdekeinek biztosítására megfelelő és konkrét intézkedéseket ír elő.⁴⁷⁸

A GDPR 22. cikkének rendelkezései képezik az EU – kizárólag automatizált adatkezelésen alapuló döntéshozatallal kapcsolatos – álláspontjának gerincét, és további jogszabályok szemléletének kiindulópontjául szolgáltak. Ez az egyik legfajsúlyosabb érintetti jog, ami megelőlegezte azokat a tilalmakat, amelyeket a UPC-irányelv a manipulatív gyakorlatokkal, a DSA a sötét megoldásokkal és a DMA a kapuőrök piaci erőfölényével

⁴⁷³ WP259. 21–22.

⁴⁷⁴ GDPR (71) preambulumbekzdés és 22. cikk (2)–(3) bekezdés

⁴⁷⁵ ECLI:EU:C:2023:957. A Bíróság (első tanács) ítélete a C-634/21. sz. (SCHUFA, automatizált döntéshozatal hitelminősítésnél) ügyben, 2023. december 7. 75. pont

⁴⁷⁶ GDPR 22. cikk (3) bekezdés

⁴⁷⁷ Nils LÖLFING: *CJEU confirms preparatory acts can be automated individual decisions: the SCHUFA cases*. Bird & Bird 2023. https://www.twobirds.com/en/insights/2023/global/key-takeaways-from-the-schufa-case-of-the-cjeu?utm_source=chatgpt.com (letöltés: 2025. 01. 05.)

⁴⁷⁸ GDPR 22. cikk (4) bekezdés

kapcsolatban tartalmaz. Nemcsak adatvédelmi kockázatot hordoz tehát, hanem a piacra is és a fogyasztókra is hatással lehet. A DMA a kapuőröket fékezi abban, hogy algoritmikus eszközökkel korlátozzák a tisztességes versenyt, az átláthatóságot célozzák a fogyasztókról készült profilalkotásra használt technikák auditált leírásával összefüggő szabályok. A DSA-ben az algoritmikus döntéshozatalnak az ajánlórendszerek, a tartalommoderálás, a szintén algoritmusokkal megvalósuló sötét megoldások vonatkozásában van szerepe, valamint a beépített megfelelés (compliance by design) követelménye is automatizált folyamatokat foglal magában.⁴⁷⁹ Az automatizált döntéshozatal tekintetében a DSA és a DMA a platformok működésére vonatkozóan egészítik ki és részletezik az átláthatósági követelményeket, de ezek nem alkotnak egységes, koherens és átfogó szabályrendszert.⁴⁸⁰

A digitális omnibusz csomag javaslata azzal, hogy szerződéskötéshez és -teljesítéshez lehetővé teszi az algoritmikus döntéshozatalt még akkor is, ha a döntés nem kizárólag automatizált módon hozható meg,⁴⁸¹ gyengítheti az érintettek védelmét. Különösen a pénzügyi szolgáltatások területén foszthatja meg a fogyasztókat az automatizált döntéshozattal szembeni védelem lehetőségétől.

4.9. A GDPR érintetti jogai és a fogyasztóvédelmi jog összefüggései

Dolgozatom VI. fejezete a fogyasztóvédelem eszközrendszerét mutatja be a személyes adatokkal összefüggésben, ezért a jelen fejezetben tárgyalt érintetti jogokat fogyasztóvédelmi összefüggésbe helyezem, előrevetítve néhány rendelkezés jelentőségét. Ez határozta meg a 3. táblázatba felvett fogyasztóvédelmi uniós jogszabályokat. A táblázatban rámutatok azokra a kapcsolódási pontokra, amelyek e két jogterület analógiáját jelzik. A két jogterület eltérő eszközökkel operál, mégis azonos cél elérésére törekszik: az erősebb féllel szemben a kiszolgáltatottság csökkentésére.

3. táblázat: GDPR szerinti érintetti jogok és azok funkcionális párhuzamai az uniós fogyasztóvédelmi jogban

GDPR szerinti érintetti jog (12–22. cikk)	Fogyasztóvédelmi kapcsolódási pont	Fogyasztóvédelmi párhuzam, analógia és cél
Átlátható tájékoztatás és a tájékoztatáshoz való jog	CR-irányelv 5–6. cikk	Szerződéskötést megelőző kötelező tájékoztatás: az információs aszimmetria felszámolása a szerződéses feltételek és a kereskedő adatainak rögzítésével
	UCP-irányelv 7. cikk	Megtévesztő mulasztások tilalma: az érdemi ügyleti döntéshez szükséges lényeges információk elhallgatása tilos

⁴⁷⁹ DSA 27. cikk, 14–15. cikk, 25. cikk, 31. cikk

⁴⁸⁰ ELI i. m. 7.

⁴⁸¹ Digitális omnibusz csomag javaslata 3. cikk 7. pont

	DCS-irányelv 7. cikk	A szerződésszerűség szubjektív követelményei: tájékoztatás a digitális tartalom/szolgáltatás tulajdonságairól, ami a szerződésszerű teljesítés alapja
Hozzáférési jog	CR-irányelv 8. cikk (7) bekezdés	A jogviszony tartalmának rögzítése: a kereskedő köteles a megkötött szerződésről tartós adathordozón visszaigazolást adni, biztosítva a fogyasztó utólagos ellenőrzési jogát
	DCS-irányelv 16. cikk (4) bekezdés	Hozzáférés saját adatokhoz: a szolgáltatott vagy generált tartalom lehívásának joga a szerződés megszűnése után
Helyesbítéshez való jog	DCS-irányelv 14. cikk	Hibás teljesítés orvoslása: a digitális szolgáltatás hibás teljesítésének szerződésszerűvé tétele (kijavítása)
Törléshez való jog (elfeledtetés)	DCS-irányelv 16. cikk (3) bekezdés	Adatfelhasználás megszüntetése: a kereskedő a szerződés megszűnése után köteles tartózkodni a fogyasztó által szolgáltatott tartalom további használatától
	CR-irányelv 9–14. cikk	Elállási jog: a fogyasztó egyoldalúan és indoklás nélkül elállhat a szerződéstől
Adatkezelés korlátozásához való jog	CR-irányelv 13. cikk	Visszatérítés visszatartása: a kereskedő visszatarthatja a visszatérítést, amíg az árut vissza nem kapja vagy a visszaküldés igazolása meg nem történik
	DCS-irányelv 14. cikk (4) bekezdés	Ellenszolgáltatás arányos mérséklése: a fogyasztó visszatarthatja az ellenszolgáltatást a digitális tartalom szerződésszerűvé tételéig
Adathordozhatósághoz való jog	(DCS-irányelv 16. cikk (4) bekezdés)	(Nincs valódi adathordozhatóság, csak passzív hozzáférés, csak részleges analógia van: a szerződés megszűnése után a fogyasztó csak lehívni tudja a digitális tartalmakat)
Tiltakozáshoz való jog	CR-irányelv I. melléklet 26. pont	Kéretlen megkeresések tilalma: a fogyasztó joga, hogy a nem kívánt, sürgető megkereséseknek véget vessen (agresszív gyakorlat tilalma)
Automatizált döntéshozatal és profilalkotás	UCP-irányelv 5. cikk	Manipulatív befolyásolás tilalma: a kiszolgáltatott fogyasztót kihasználó tisztességtelen gyakorlatok elleni védelem
	DSA 25. cikk	Megtevesztő és manipulatív interfészek tilalma: a felhasználói felületek olyan kialakításának tilalma, amely torzítja a szabad és tájékozott döntéshozatalt
	DSA 27. cikk	Ajánlórendszerek átláthatósága: a profilalkotáson alapuló algoritmusok fő paramétereinek közzététele és a felhasználó általi módosíthatósága

Forrás: saját szerkesztés HELBERGER–BORGESIU–REYNA *i. m.* (pdf) alapján, valamint a táblázatban feltüntetett jogszabályok alapján

A táblázat alapján azt látjuk, hogy GDPR érintetti jogai – a funkciójuk tekintetében – több ponton megfeleltethetők az uniós fogyasztóvédelmi rendelkezéseknek, aminek a gyengébb fél védelme az alapja. Azt is mondhatjuk, hogy hasonló pozíciót kezelnek hasonló védelmi mechanizmussal, de közös cél mentén. Az uniós polgárok szempontjából a kapcsolódási pontok azt a védőhálót erősítik, ami a kiszolgáltatottságuk csökkentését célozza, míg a közösségi jogalkotás szempontjából a belső koherencia igényével való fellépés példája. Az adatvédelem nem különálló, nem elszigetelt terület, a klasszikus fogyasztóvédelem eszközrendszerét, mechanizmusait alkalmazza, de ezeket a digitális térre formálja át; ebben az értelemben a GDPR korszerűsített formában reagál a gazdaság szabálytalanságára, egyenatlenségeire, kiterjesztve a fogyasztói autonómia kereteit. Hogy az ember ne csupán adathalmaz és

adatösszefüggés legyen, ahhoz az kell, hogy folyamatosan kontrollálni tudja a burjánzó, mindent átszövő adatfelhasználást, megőrizve autonómiáját, önrendelkezését. A kérdés az, hogy az adatvezérelt vállalatokkal szemben képes-e a gyakorlatban is érvényesíteni e jogokat.

5. Az adatkezelés alapvető elvei

Míg az érintettek önrendelkezésére épülő érintetti jogok aktivitást feltételeznek és kívánnak meg, addig a GDPR-nak van egy olyan pillére, amely az adatkezelő felelősségére építve preventív rendelkezéseket tartalmaz. Idetartoznak az adatkezelés alapvető elvei, amelyek egy részét a GDPR-t megelőző adatvédelmi jogszabályok – más néven, vagy más hangsúllyal – már szintén tartalmazták; ezeket összegzi az alábbi, 4. táblázat.

4. táblázat: Az adatkezelés alapelvei

A SZEMÉLYES ADATOK KEZELÉSÉRE VONATKOZÓ ELVEK (GDPR 5. CIKK)	AZ ELVEK JELENTÉSE
- jogszerűség, - tisztességes eljárás - és átláthatóság	- jogalapnak megfelelő adatkezelés - adatkezelő–érintett viszonyban → az emberi méltóság védelme (pl. titkos adatgyűjtés, megfélemlítés tilos) - az adatkezelés folyamata és dokumentáltsága az érintett számára megismerhető, a tájékoztatás érthető, egyértelmű, könnyen hozzáférhető
célhoz kötöttség	egyértelmű és jogszerű cél meghatározása → a személyes adatok kezelése csak e céllal összeegyeztethető módon
adattakarékosság	annyi és olyan személyes adat kezelhető, ami szükséges és elégséges az adatkezelési cél megvalósításához
pontosság	a kezelt adatoknak pontosnak (valóságnak megfelelőnek) és naprakésznek kell lenniük (a pontatlan személyes adatokat törölni/helyesbíteni kell)
korlátozott tárolhatóság	ha már nincs szükség a személyes adatra abból a célból, amire eredetileg gyűjtötték → törölni vagy anonimizálni kell
integritás és bizalmas jelleg (– adatbiztonság)	az adatkezelést úgy kell végezni, hogy – megfelelő technikai vagy szervezési intézkedésekkel – az adatok biztonsága biztosított legyen (jogosulatlan vagy jogellenes kezelés, véletlen elvesztés, megsemmisítés, károsodás elleni védelem)

Forrás: saját szerkesztés a GDPR 5. cikke alapján és a korábbi adatvédelmi jogszabályok alapján

Az alapelvek másik csoportja – mivel a digitális környezettel összefüggésben az adatkezelés pontosabb módszerek és jogi eszközök fajsúlyos megjelenítését igényli – új elemként jelent meg a GDPR-ban, ilyen a beépített és alapértelmezett adatvédelem, valamint az adatvédelmi hatásvizsgálat.

5.1. Beépített és alapértelmezett adatvédelem

A beépített és alapértelmezett adatvédelem nem szerepel a személyes adatok kezelésére vonatkozó, 5. cikkben felsorolt elvek között, hanem egy önálló cikk, a 25. foglalkozik vele.⁴⁸²

⁴⁸² GDPR 25. cikk

A két cikk között szoros kapcsolat van, utóbbi a hogyan kérdésre válaszol, vagyis hogy az elveket hogyan kell a folyamatok tervezésekor és működtetésekor konkrétan megvalósítani.

Az európai adatvédelmi biztos már 2010-ben⁴⁸³ felhívta a figyelmet arra, hogy az IKT a társadalom számára nemcsak előnyökkel, de a magánélet és az adatok védelmére vonatkozó kockázatokkal is jár. Az IKT iránti bizalom megteremtésének fő eszközeként a beépített adatvédelem (Privacy by design) elvét nevezte meg, amelynek a jogi keretbe illesztése révén az uniós polgárok az online térben egyre nagyobb biztonságban érezhetik majd magukat. Lényege, hogy „a magánélet és az adatok védelmét a technológia teljes életciklusába beépítsék, a legkorábbi tervezési szakasztól kezdve a végső üzembe helyezésig, felhasználásig, majd ártalmatlanításig.”⁴⁸⁴ A beépített adatvédelemnek az adatvédelmi irányelvben tetten érhető annyi előzménye, hogy a személyes adatok megsemmisülése, megváltoztatása, jogosulatlan nyilvánosságra hozatala elleni védelem érdekében az adatkezelők megfelelő technikai és szervezési intézkedéseket hajtsanak végre,⁴⁸⁵ ami a gyakorlatban nem bizonyult elegendőnek, ezért a biztos általános elvként javasolta bevezetni az adatvédelmi jogi keretbe.⁴⁸⁶

Míg korábban a vállalkozások, szervezetek rutinból alkották meg vagy másolták egymás adatkezelési dokumentumait, ez a GDPR kötelező alkalmazása során nem fordulhat elő, hiszen az adatkezelőnek az adott szervezetre kell szabnia, az egyedi sajátosságok, jellemzők alapján kell kidolgoznia az adatkezelés rendszerét. A beépített adatvédelem követelménye azt jelenti, hogy az adatkezelő úgy tervezi meg és alakítja ki az adott szervezet adatkezelési módját, hogy egyrészt figyelembe veszi a tudomány, a technológia állását, a költségeket, az adatkezelés jellegét, hatókörét, körülményeit és céljait; másrészt elemzi, azonosítja és figyelembe veszi a természetes személyek jogaira jelentett kockázatokat; ideértve a megfelelő garanciák és jogalapok jelentőségét is. Az előzetes tervezés szempontjai: „a GDPR alapelveinek – különösen a célhoz kötöttség és a jogszerűség elvének – megfelelő működés; az érintett jogainak biztosítására szolgáló mechanizmusok kialakítása; az adatbiztonság, ill. az integritás és bizalmas jelleg garantálása.”⁴⁸⁷ A beállítások akár gyárilag is lehetnek beágyazottak, vagy konfigurálással is előállíthatók, bár „az informatikai infrastruktúra átalakítása [...] jelentős költségekkel jár.”⁴⁸⁸ A GDPR az adatkezelő által végrehajtandó technikai és szervezési

⁴⁸³ 2010/C 280/01. Az európai adatvédelmi biztos véleménye az információs társadalom iránti bizalomnak az adatok és a magánélet védelme elősegítése révén történő erősítéséről

⁴⁸⁴ 2010/C 280/01. 19. pont

⁴⁸⁵ Adatvédelmi irányelv 17. cikk

⁴⁸⁶ 2010/C 280/01. 40. pont

⁴⁸⁷ G. KARÁCSONY Gergely: *Adatvédelmi szabályozás*. In: FARKAS Ádám – KELEMEN Roland (szerk.): *Kibertér és biztonság egyes jogtani és államtani kérdései*. Győr, Universitas-Győr Nonprofit Kft., 2024. 292.

⁴⁸⁸ BÖRÖCZ István – SZÖKE Gergely László: *A beépített adatvédelem (Privacy by Design) elve*. Infokommunikáció és Jog 2013/3. 120.

intézkedésekre vonatkozóan egyetlen példát említ, az álnevesítést,⁴⁸⁹ de ehhez az EDPB hozzáteszi, hogy „lehet bármi a fejlett technikai megoldások használatától kezdve a személyzet alapképzéséig,” így jelszavak, biztonsági mentések, beépített adattörlési eljárások stb.⁴⁹⁰

Az adatvédelmi biztosok jeruzsálemi konferenciája már 2010-ben kiemelte, hogy a beépített adatvédelmet holisztikusan kell figyelembe venni, a tervezéstől az üzemeltetésen át a termékek és szolgáltatások teljes életciklusára vonatkozóan.⁴⁹¹ A 29. cikk alapján létrehozott adatvédelmi munkacsoport pedig már 2009-ben úgy foglalt állást, hogy a beépített adatvédelem elvének nemcsak az adatkezelőkre, hanem a technológiai tervezőkre és gyártókra is kötelező érvényűnek kell lennie,⁴⁹² hiszen a tervezők és gyártók tudják alapvetően meghatározni a termékek, a szolgáltatások funkcióit, és a személyesadat-védelem betartása úgy garantálható leginkább, ha az már a létrehozáskor beágyazódik a technológiába. Ez alapján azt várnánk, hogy a beépített adatvédelem egységesen fogalmazódik meg az európai adatvédelmi jogszabályokban. De nem így van, hiszen még a 2016-ban hatályba lépett GDPR is csak az adatkezelőkre ró kötelezettségeket, a gyártókra, termék-előállítókra, szoftverfejlesztőkre nem, ezeket csupán ösztönzi arra, hogy a termékek, szolgáltatások „tervezésekor szem előtt tartsák a személyes adatok védelméhez való jogot.”⁴⁹³

Az adatvédelem másik kulcsfogalma az alapértelmezett adatvédelem (Privacy by default), amely „meghatározott vagy előírt konfigurációs értékekkel vagy adatkezelési lehetőségekkel, például szoftveralkalmazással, szolgáltatással vagy eszközzel, vagy manuális adatkezelési eljárással kapcsolatos választásokra,”⁴⁹⁴ azaz a „konkrét működési módra,”⁴⁹⁵ a választások beállítására vonatkozik. Az adatkezelőnek oly módon kell megválasztania az adatkezelés beállításait, hogy alapértelmezés szerint kizárólag a meghatározott, jogszerű cél eléréséhez feltétlenül szükséges adatkezelésre kerüljön sor. Eszerint kizárólag olyan személyes adatok kezelésére kerülhet sor, amelyek az adott adatkezelési cél szempontjából szükségesek, vagyis a személyes adatok alapértelmezés szerint – a természetes személy beavatkozása nélkül

⁴⁸⁹ GDPR 25. cikk (1) bekezdés

⁴⁹⁰ EDPB: 4/2019. 9. pont és NAIH STAR-projekt: 7. témakör – Technikai és szervezési intézkedések. 22–23. dia. <https://www.naih.hu/star-i/stari-eredmenyek> (letöltés: 2023. 02. 02.)

⁴⁹¹ 32nd International Conference of Data Protection and Privacy Commissioners Jerusalem, Israel 27-29 October, 2010. Resolution on Privacy by Design. <https://globalprivacyassembly.org/wp-content/uploads/2015/02/32-Conference-Israel-resolution-on-Privacy-by-Design.pdf> (letöltés: 2022. 01. 12.)

⁴⁹² Wp168. Article 29 Data Protection Working Party: The Future of Privacy. Joint contribution to the Consultation of the European Commission on the legal framework for the fundamental right to protection of personal data. Adopted on 01 December 2009. 3.

⁴⁹³ GDPR (78) preambulumbekkezdés

⁴⁹⁴ EDPB: 4/2019. 41. pont

⁴⁹⁵ G. KARÁCSONY (2024) i. m. 292.

– ne válhassanak más személy számára hozzáférhetővé.⁴⁹⁶ Az alapértelmezett beállítások a legszigorúbb védelmet automatikusan biztosítják az érintettek számára, ugyanis többségük nem változtatja meg ezeket, mivel sem idejük, sem szaktudásuk nincs a tudatos módosításokhoz. Különösen kulcsfontosságúak a fogyasztók számára, mert az alapértelmezett adatvédelmi beállítások határozzák meg a fogyasztói döntéshozatalt, s ha a beállítások a jogszabályok által elvárt védelmi szintet tükrözik, akkor a tisztességes döntési környezet is biztosított.

A konkrét megvalósításra példaként említhetők a valamely pályázati kiírásra érkezett anyagok, amelyek személyes adatokat tartalmaznak. A nyertes pályázatok esetében jogszabályban meghatározottak szerint történik az adatkezelés, a beépített és alapértelmezett adatvédelem alapján beállítható például a hozzáférési jogosultság. A nem nyertes pályázatokhoz kapcsolódó személyes adatokat törölni vagy anonimizálni kell, ami megoldható előre meghatározott és beágyazott paraméterek segítségével: a számítógép (feladatütemező) a pályázati döntést követően felkínálja a nem nyertes pályázathoz kapcsolódó adatok törlésének lehetőségét, amit ha nem végeznek el, újabb meghatározott idő elteltével maga törli vagy anonimizálja azokat. Ugyanígy a vállalat által hirdetett állásra a jelentkezők által küldött önéletrajzok, motivációs levelek tárolása kapcsán is, ha megszűnik a jogalap, vagyis a felvételi eljárás, az adatokat sem szabad tovább tárolni, erre vonatkozóan is tehetők technikai intézkedések. A GDPR előírásai alapján az adatkezelés teljes folyamata meghatározott rend, tervezés alapján kell történnjen, amit az adatkezelőnek kell átgondolnia és felépítenie.

A beépített és alapértelmezett adatvédelem a technikai kialakítás és beállítások révén fogyasztóvédelmi funkcióval is rendelkezik. Egyszerűen szemlélteti ezt a következő párhuzam: farsangi jelmez vásárlása esetén rendelkezés védi a fogyasztót attól, hogy a kiegészítő terméket, például a hajpántot előre bepipált négyzettel kínálja számára a webshop; ugyanígy a GDPR is védi az érintettet azzal, hogy tiltja az előre bepipált checkbox használatát például a hozzájárulásra vonatkozóan. Ez a példa rámutat arra, hogy a két jogterület logikája ugyanaz: mindkettő a jogsértés megelőzésére törekszik, nem orvoslására; mindezt tilalom felállításával teszi; és a gyengébb fél védelme a cél. A kapcsolódási pontokra konkrét jogszabályokkal lehet rávilágítani. A fenti példa kapcsolódási pontja az, hogy alapértelmezett beállításként tilos az előre bepipált négyzetek használata. A CR-irányelv szerint a fogyasztóra nem lehet további fizetési költséget terhelni alapértelmezett opciók alapján, ehhez annak kifejezett hozzájárulása szükséges; a GDPR alapján az adatkezelő sem kényszerítheti ki a beleegyezést, mert annak önkéntesnek kell lennie.⁴⁹⁷

⁴⁹⁶ GDPR 25. cikk (2) bekezdés

⁴⁹⁷ CR-irányelv 22. cikk; GDPR 4. cikk 11. pont, 7. cikk, (32) preambulumbekkezdés

Egy további kapcsolódási pont a sötét megoldások kezelése, amely mind a fogyasztóvédelmi, mind az adatvédelmi jogban megjelenik. A UCP-irányelv tiltja a fogyasztói döntéseket befolyásoló agresszív kereskedelmi gyakorlatokat, a DSA az olyan interfészalkalakat tiltja, amelyek manipulatív vagy megtévesztő módon befolyásolják a felhasználók döntéseit,⁴⁹⁸ s ezekhez azzal kapcsolódik a GDPR, hogy előírja: technikai-szervezési intézkedésekkel kell biztosítani, hogy csak a konkrét adatkezelési cél szempontjából szükséges személyes adatok legyenek gyűjthetők. Nem arról van szó, hogy mindhárom jogforrás ugyanazt a magatartást kezelné – mert mindháromnak más a szabályozási fókusz –; hanem arról, hogy héjazatszerűen egymásra épülnek a szabályozási rétegek, és együttesen járulnak hozzá a felhasználói, fogyasztói döntések védelméhez.⁴⁹⁹

Kapcsolódási pont azonosítható a UCP-irányelv és a GDPR vonatkozásában: előbbi a fogyasztó gazdasági magatartását befolyásoló kereskedelmi gyakorlatokat tiltja, utóbbi olyan beépített és alapértelmezett megoldásokat használ, amelyek az érintett döntéseit tisztességes környezetté alakítva segítik.⁵⁰⁰ Mindkettő strukturális szinten gondolkodik, nem az egyedi szerződésekre vonatkozóan, és nem az egyes érintettek vonatkozásában, hanem a gyakorlat egészének kialakításával.

A bemutatott párhuzamok arra világítanak rá, hogy a GDPR beépített és alapértelmezett adatvédelem elve – funkcióját tekintve – a fogyasztóvédelmi eszközökkel rokon. A rokonságot főleg az ex ante szabályozás területei bizonyítják: a tisztességtelen kereskedelmi gyakorlatok tilalma, a sötét megoldások elleni fellépés és az információs aszimmetria csökkentése.

5.2. Az elszámoltathatóság elve

A beépített és alapértelmezett adatvédelem elve szorosan kapcsolódik az elszámoltathatóság elvéhez. Előzményeként említhető a felelősségre vonhatóság elve, amely már az OECD-irányelvben is megjelent,⁵⁰¹ és az Infotv. is utal rá.⁵⁰² Ehhez képest a GDPR az elszámoltathatóság elvét alapvető szintre emelte, és középponti szerepet adott neki, ezért emlegetik szuperalapelvként.⁵⁰³ Az elszámoltathatóság két elemet foglal magában: az

⁴⁹⁸ UCP-irányelv (8)–(9) cikk; DSA 25. cikk

⁴⁹⁹ DSA 25. cikk (2) bekezdés

⁵⁰⁰ UCP-irányelv (5)–(7) cikk; GDPR 25. cikk

⁵⁰¹ OECD-irányelvek 14. pontja: „Az adatellenőrző legyen felelősségre vonható, hogy azon intézkedések szerint jár-e el, melyek a fenti alapelveknek érvényt szereznek.”

⁵⁰² Infotv. 23. §: „mindenki, aki jogellenes adatfeldolgozási művelet vagy az ezen irányelv értelmében elfogadott nemzeti rendelkezésekkel összeegyeztethetetlen intézkedés eredményeképpen kárt szenvedett, az adatkezelőtől kártérítésre jogosult az elszenvedett kárért.”

⁵⁰³ PÓK László: *Az adatvédelem „szuperalapelve” – az elszámoltathatóság*. Blogbejegyzés. 2017. június 14. http://gdpr.blog.hu/2017/06/14/az_adatvedelem_szuperalapelve_az_elszamoltathatosag (letöltés: 2018. 05. 03.)

adatkezelő felelősségévé teszi a személyes adatok kezelésére vonatkozó elvek érvényesítését,⁵⁰⁴ melynek érdekében ki kell alakítania „a belső szabályokat, folyamatokat, mechanizmusokat,”⁵⁰⁵ és mindezeket igazolni kell tudnia. Az adatkezelő vagy az adatfeldolgozó oly módon tudja igazolni az általa végzett és a felelősségébe tartozó adatkezelési tevékenységeket, ha azokról – írásban, ideértve az elektronikus formát is⁵⁰⁶ – nyilvántartást vezet. Ellenőrzés során mind az adatkezelő, mind az adatfeldolgozó köteles a felügyeleti hatósággal együttműködni, és ennek során ezeket a nyilvántartásokat hozzáférhetővé tenni.⁵⁰⁷

A GDPR nem egységes terhet ró minden adatkezelőre. A nyilvántartás-vezetési kötelezettség a 250 főnél kevesebb személyt foglalkoztató szervezetre csak abban az esetben vonatkozik, ha az általa végzett adatkezelés az érintettek jogaira és szabadságaira nézve valószínűsíthetően kockázattal jár, vagy ha kiterjed a személyes adatok különleges kategóriáinak vagy büntetőjogi felelősség megállapítására vonatkozó határozatokra és bűncselekményekre vonatkozó személyes adatoknak a kezelésére.⁵⁰⁸ Ezt a rendelkezést kivéve a GDPR nem veszi figyelembe a vállalkozások közötti erőforrás-különbségeket, így a kkv-k számára arányaiban nagyobb gazdasági és adminisztratív terhet jelent a betartása, tehát „egyenlőtlen versenyhelyzetet teremthet,”⁵⁰⁹ és ezáltal a fogyasztókra is hatással lehet. Bár most folyik a jogalkotási egyeztetés a létszámhatár 500, esetleg 750 főre emeléséről,⁵¹⁰ véleményem szerint ez csak kevés egyszerűsítést jelent, az anyagi és adminisztratív terheken nem enyhít, különösen, ha figyelembe vesszük, hogy jogi, technikai és anyagi háttérrel a nagy platformok sokkal könnyebben tudnak megfelelni az előírásoknak.

6. Az adatvédelmi hatásvizsgálat

A személyes adatok kezeléséből a természetes személyek jogait és szabadságait érintő, fizikai, vagyoni vagy nem vagyoni károkat okozó kockázatok származhatnak.⁵¹¹ Az adatvédelmi hatásvizsgálat alapvető célja az, hogy az adatvédelmi hiányosságokat feltárja, még

⁵⁰⁴ GDPR 5. cikk (2) bekezdés

⁵⁰⁵ SZABÓ Endre Győző: *Az Európai Unió általános adatvédelmi rendeletének egyes kérdéseiről, II.: Beépített és alapértelmezett adatvédelem – Adatvédelmi incidensek bejelentése*. Pázmány Law Working Papers 2016/27. 4. https://plwp.eu/docs/wp/2016/2016-27_Szabo.pdf (letöltés: 2019. 01. 04.)

⁵⁰⁶ GDPR 30. cikk (3) bekezdés

⁵⁰⁷ GDPR (82) preambulumbekkezdés

⁵⁰⁸ GDPR 30. cikk (5) bekezdés

⁵⁰⁹ KOPPÁNY Zsombor: *A GDPR piaci hatásai*. 2019. <https://arsboni.hu/a-gdpr-piaci-hatasai/> (letöltés: 2025. 12. 10.)

⁵¹⁰ EDPB.EUROPA.EU: *Az általános adatvédelmi rendelet célzott módosításai*: EDPB & az európai adatvédelmi biztos üdvözlí a nyilvántartási kötelezettségek egyszerűsítését, és további pontosítást kér. Sajtóközlemény, Brüsszel, 2025. július 9. https://www.edpb.europa.eu/news/news/2025/targeted-modifications-gdpr-edpb-edps-welcome-simplification-record-keeping_hu (letöltés: 2025. 10. 12.)

⁵¹¹ GDPR (75) preambulumbekkezdés

az adatkezelés megkezdése előtt. Az adatkezelőnek meg kell állapítania, hogy a tervezett adatkezelési műveletek a személyes adatok védelmét hogyan érintik, a kockázatokat fel kell tárnia, be kell azonosítania, forrásukat, jellegüket, valószínűségüket és súlyosságukat fel kell mérnie, és a mérséklésükre szolgáló intézkedéseket kell tennie.⁵¹² A GDPR különbséget tesz kockázat és magas kockázat között. A kockázat valószínűségét és súlyosságát objektív értékelés alapján kell felmérni,⁵¹³ ebben segítséget nyújtanak a jóváhagyott magatartási kódexek, tanúsítási eljárások, az adatvédelmi tisztviselő és a 29. cikk szerinti munkacsoport iránymutatása. A magas kockázat kezelésére a rendelet új jogintézményt vezet be, az adatvédelmi hatásvizsgálatot. A hatásvizsgálat az adatkezeléssel kapcsolatos döntések meghozatalát segíti,⁵¹⁴ az adatkezelést megelőzően kell elvégezni,⁵¹⁵ és hozzájárul a beépített és alapértelmezett adatvédelem elvének érvényesüléséhez.

Valószínűsíthetően magas kockázattal jár? – erre a kérdésre minden adatkezelőnek választ kell adnia, ez alapján arról születik döntés, hogy szükséges-e az adatvédelmi hatásvizsgálat elvégzése. A GDPR szerint akkor kell elvégezni, ha az adatkezelés valószínűsíthetően magas kockázattal jár, és felsorolja azokat az eseteket, amikor kötelező a hatásvizsgálat: a személyes jellemzők automatizált adatkezelésen alapuló módszeres és kiterjedt értékelése; a nyilvános helyek nagymértékű megfigyelése; a személyes adatok különleges kategóriáinak és/vagy a büntetőjogi felelősség megállapítására vonatkozó határozatokra és büncselekményekre vonatkozó személyes adatok nagy számban történő kezelése.⁵¹⁶ A GDPR előírja a tagállami felügyeleti hatóságok számára, hogy állítsák össze azon adatkezelési művelet típusok jegyzékét, amelyek esetében kötelező az adatvédelmi hatásvizsgálat elvégzése;⁵¹⁷ de a nem kötelező esetek jegyzékét is összeállíthatják.⁵¹⁸

A 29. cikk alapján létrehozott adatvédelmi munkacsoport – az eredendően magas kockázatuk miatt kötelező adatvédelmi hatásvizsgálat hatálya alá tartozó adatkezelési műveletek körének pontosabb meghatározása érdekében – kilenc mérlegelendő szempontot mutat be. Az előbbieken felsorolt kötelező esetekhez kapcsolódó szempontokon túl az új technológiai vagy szervezési megoldások innovatív használata az egyik szempont,⁵¹⁹ amelynek

⁵¹² GDPR (76), (77) és (83) preambulumbekkezdés

⁵¹³ GDPR (76) preambulumbekkezdés

⁵¹⁴ WP248. A 29. cikk alapján létrehozott adatvédelmi munkacsoport: Iránymutatás az adatvédelmi hatásvizsgálat elvégzéséhez és annak megállapításához, hogy az adatkezelés az (EU) 2016/679 rendelet alkalmazásában „valószínűsíthetően magas kockázattal jár”-e. 17.

⁵¹⁵ GDPR 35. cikk (1) és (10) bekezdés

⁵¹⁶ GDPR 35. cikk (1) és (3) bekezdés

⁵¹⁷ GDPR 35. cikk (4) bekezdés. Magyarországon: NAIH: GDPR 35. cikk (4) bekezdése alapján összeállított jegyzék: https://naih.hu/files/GDPR_35_4_lista_HU_mod.pdf (letöltés: 2022. 03. 02.)

⁵¹⁸ GDPR 35. cikk (5) bekezdés

⁵¹⁹ WP248. 10–12.

a felgyorsult technológiai fejlődés miatt fokozott jelentősége van. Példaként említhetők az IoT-t használó alkalmazások, mert az adatok követhetetlenül vándorolnak személyek, eszközök és rendszerek között, ezért a személyes adatok biztonsága olyan intézkedéseket kíván az adatkezelőktől, amelyeket a feltárt kockázatok alapján majd meg kell terveznie.⁵²⁰

Az adatvédelmi hatásvizsgálat szükségességének eldöntése után kerül sor magára a vizsgálatra, az elemzésre, melynek tartalmát a GDPR határozza meg. A tartalmi jellemzők számbavétele egyúttal – mivel a rendelet külön nem definiálja a fogalmat – az adatvédelmi hatásvizsgálat definíciójának is tekinthető. Felöleli a tervezett adatkezelési műveletek módszeres leírását és az adatkezelés céljainak ismertetését; az adatkezelési műveletek szükségességi és arányossági vizsgálatát; az érintett jogait és szabadságait érintő kockázatok vizsgálatát; valamint a kockázatok kezelését célzó intézkedések bemutatását.⁵²¹ Ha a folyamat végére a fennmaradó kockázatok továbbra is jelentősek, szükséges konzultálni a felügyeleti hatósággal. Az adatvédelmi hatásvizsgálat végrehajtásáról az adatkezelő gondoskodik, egyúttal felelős a teljesítéséért. Ha van, az adatvédelmi tisztviselő tanácsát ki kell kérnie.⁵²² A hatásvizsgálatot érdemes folyamatosan felülvizsgálni, erre leginkább az adatkezelés körülményeinek változása vagy az ebből eredő kockázatok megváltozása miatt van szükség;⁵²³ illetőleg ellenőrizni kell, hogy a személyes adatok kezelése a hatásvizsgálatnak megfelelően történik-e.⁵²⁴ (Az adatvédelmi hatásvizsgálat folyamatának lépéseit a 4. melléklet tartalmazza.)

Korunkban szinte semmilyen rendszer nem képes teljes biztonságot garantálni a személyes adatok védelme tekintetében. A GDPR megszabja azokat a lépéseket, amelyeket adatvédelmi incidens esetén – „a biztonság olyan sérülése, amely a továbbított, tárolt vagy más módon kezelt személyes adatok véletlen vagy jogellenes megsemmisítését, elvesztését, megváltoztatását, jogosulatlan közlését vagy az azokhoz való jogosulatlan hozzáférést eredményezi”⁵²⁵ – az adatkezelőnek tennie kell. A nyilvántartások és értesítések három szintje különböztethető meg: az adatkezelő házon belüli nyilvántartása az ellenőrzések végett; a hatóság tájékoztatása; és a nyilvánosság tájékoztatása az incidens körülményeiről.⁵²⁶ Az adatvédelmi incidenst a felügyelő hatóságnak indokolatlan késedelem nélkül, ha lehetséges,

⁵²⁰ ESZTERI Dániel: *Az új technológiák megjelenésének hatása a személyes adatok védelmére: gépi tanulás, blokklánc, internet-of-things, agyhullám-olvasás.* 16.
<https://real.mtak.hu/133906/1/eszteri.daniel.uj.technologiak.adatvedelem.pdf> (letöltés: 2022. 03. 02.)

⁵²¹ GDPR 35. cikk (7) bekezdés

⁵²² GDPR 35. cikk (2) bekezdés

⁵²³ WP248. 16.

⁵²⁴ GDPR 35. cikk (11) bekezdés

⁵²⁵ GDPR 4. cikk 12. pont

⁵²⁶ SZABÓ Endre Győző (2016) i. m. 5.

legkésőbb 72 órával⁵²⁷ az után, hogy az adatkezelő tudomására jutott, kell bejelenteni. Az adatvédelmi incidensek körébe tartoznak: a téves címzett részére küldött e-mailek, a több címzett részére küldött e-mailek esetében a címzettek felsorolása a „másolatot kap” mezőben, az elveszett vagy ellopott telefonok, laptopok, valamint a hackertámadások. A digitális omnibusz csomag javaslata szerint a bejelentési kötelezettség határideje 96 órára emelkedne, és csak a magas kockázatú eseteket kellene jelenteni, amelyekről az EDPB listát állít össze az értesítési küszöbérték alapján. Tervek szerint jelentéstételre szolgáló egyablakos ügyintézési pontot hoznak létre.⁵²⁸ Ezek a javaslatok az adatkezelő adminisztratív terheit kívánják csökkenteni. Az incidenseket központi uniós adatbázisban vezetnék, ami segíti a kockázatos adatkezelések azonosítását, ideértve a határokon átnyúló támadásokat is.

Véleményem szerint az adatvédelmi hatásvizsgálat legfőbb értéke a kockázatelemző és ebből következően a megelőző funkciója, aminek alapos tervezéssel kell összekapcsolódnia. A szabályozás gyenge pontjának tartom azonban, hogy a vonatkozó rendelkezések megfogalmazása több bizonytalan jelentésű szót és szókapcsolatot tartalmaz (jelentős, nagy számban stb.), és a 29. cikk alapján létrehozott adatvédelmi munkacsoport iránymutatása sem közöl egyértelmű viszonyítási pontokat ezek értelmezéséhez.⁵²⁹ Továbbá, miután az adatkezelő saját szempontsor alapján önmaga végzi a hatásvizsgálatot, és – ha nem vesz részt előzetes konzultáción – nincs kötelező kontroll, legfeljebb a hatóság utólagos vizsgálata; addig azonban az adatkezelő akár mélyreható tervezés nélkül, formális megfelelési kötelezettségként is tekinthet a hatásvizsgálatra. Ha azonban tervszerűen és felelősséggel végzi – mint az adatkezelős ex ante kötelezettsége –, az önszabályozás fontos területévé válhat, és hatékony eszköze lehet az érintetti adatok védelmének.

7. Összegzés és következtetések

Feltérképezve a GDPR szerinti érintetti jogok és az uniós fogyasztóvédelmi jog kapcsolódási pontjait, megfogalmazható az a következtetés, hogy a klasszikus fogyasztóvédelem szabályozása mozgatórugóként szolgált a GDPR érintetti jogainak alakulásában, s a mindkettő fejlődésirányát motiváló közös nevező a gazdasági és információs aszimmetriák csökkentése, kiegyenlítési szándéka. Ebben az értelemben az említett rendelet is a fogyasztóvédelmi eszköztár elemei közé tartozik. Az érintetti jogok többsége már az adatvédelmi irányelvben is szerepelt, de a GDPR erősebb védelemmel, új névvel vagy új

⁵²⁷ GDPR 33. cikk (1) bekezdés

⁵²⁸ Digitális omnibusz csomag javaslata 3. cikk 8. pont

⁵²⁹ WP248

elemmel ruházta fel ezeket. Új jogintézményként jelent meg az adathordozhatósághoz való jog és a tiltakozáshoz való jog. Passzív jogot jelent az érintettet megillető védelem az automatizált döntéshozatal és a profilalkotás ellen. Megítélésem szerint ez utóbbi kulcsfontosságú az érintetti jogok között, mert algoritmusalapú megoldások sokasága vesz körül bennünket, határoz rólunk, és az átláthatatlan technológia miatt nehéz a védekezés ellene, ezért az ember–gép viszonyban az emberi méltóság megmaradásának garanciája is.

Több érintetti jog esetében a gyakorlati megvalósítás ütközik nehézségekbe, például az elfeledtetéshez való jog a harmadik felek részére megosztott adatokkal kapcsolatban, a helyesbítéshez való jog a profil helyesbítése tekintetében. A tájékoztatáshoz való jog a gyakorlatban szintén nem tudja betölteni funkcióját, aminek okaként a GDPR meghatározta rengeteg információ és az adatkezelők formális megfelelési kényszere egyaránt azonosítható. Nagyon leegyszerűsítve: a GDPR nagy mennyiségű információ átadását követeli, az adatkezelő tájékoztat erről, de ezzel mindkét fél ráterheli a felelősséget az érintetre.

Az érintetti jogok mellett az adatvédelem rendszerének másik összetevőjét a preventív jogintézmények alkotják, amelyek az adatkezelő kompetenciájába tartoznak. Idetartozik a kockázatokat értékelő adatvédelmi hatásvizsgálat, valamint a beépített és alapértelmezett adatvédelem elve. A hatásvizsgálat kockázatelemző célja által megelőző funkciót szolgál, ezért kulcseleme a tervezés. Szintén a tervezésre épít, de a teljes életcikluson át érvényesülnie kell a beépített adatvédelem elvének; az alapértelmezett adatvédelem pedig biztosítja azokat a választási lehetőségeket, amelyekkel az adott szervezet minimalizálhatja a kezelendő személyes adatok körét. E kettő egyre nagyobb szerepet kell, hogy kapjon az adatvédelemben, mert hozzájárulhatnak a tisztességes digitális környezet kialakításához.

A GDPR nemcsak az érintetti jogokat bővítette, hanem a kötelezettek körét is. A GDPR területi hatálya kiterjed minden olyan adatkezelőre, amely az EU területén belül tényleges tevékenységet végez, és személyes adatokat kezel, függetlenül a székhelyétől. Ez a területi hatály fogyasztói fókuszú, a fogyasztóvédelmi uniós joganyag normáiból építkezett, motiváló szempontja a megcélzás, az érintettek viselkedésének megfigyelése, valamint a tényleges helyzete. Ez a szemlélet a klasszikus fogyasztóvédelmi eszközöktől a GDPR-on át a DSA-ig töretlenül érvényesül, hatékonyságát azonban rontják a végrehajtási nehézségek, így az uniós képviselő intézményének korlátozott kikényszeríthetősége.

A GDPR végrehajtását nehezíti a decentralizált struktúra, a határokon átvívelő ügyekben az egyablakos ügyintézési mechanizmus nem hatékony. Különösen problémás ez az online platformok európai központjai esetében, mégsem valószínű, hogy hatékony megoldás kerekedne a problémára, mert a GDPR eljárási rendelete alig tartalmaz erre vonatkozó

rendelkezést. Sőt, az egységesség érdekében többletfeladatokat ró a fő felügyeleti hatóságra az érintett hatóságokkal való együttműködés kiaknázásával kapcsolatban. Kedvezőnek tűnik azonban a panaszbefogadhatósági követelmények harmonizációja, főleg a kollektív keresetek esetében; valamint a korai szakaszban történő rendezés lehetősége, mert csökkenti a leterhelést. Álláspontom szerint e rendelkezések azonban legfeljebb csekély mértékben fogják mérsékelni a hatóságok teendőit, de a végrehajtási problémát alapvetően nem fogják orvosolni. Azokkal a véleményekkel értek egyet, amelyek a DMA és a DSA központosított megoldása mellett érvelnek, legalábbis az adatvezérelt vállalatok esetében. A GDPR eljárási rendelete a fogyasztóvédelem fejlődési logikáját követi, ezt foglalja össze az 5. táblázat.

5. táblázat: A GDPR eljárási rendelete és a fogyasztóvédelem összefüggése

Fogyasztóvédelmi eszközrendszer	GDPR eljárási rendeletének rendelkezései
határokon átnyúló ügyek: több hatóság együttműködése	határokon átnyúló ügyek: fő felügyeleti hatóság, érintett felügyeleti hatóságok
tagállami hatóságok szerepének megtartása	
alternatív vitarendezési mechanizmusok	korai szakaszban történő rendezés lehetősége
alacsony küszöbértékű jogérvényesítés (low threshold enforcement)	panaszbefogadhatóság kritériumainak meghatározása, más adat nem kérhető a panasz befogadásához

Forrás: saját szerkesztés az érintett jogszabályok alapján

Véleményem szerint a bevezetett eljárási szabályok nem lesznek képesek ellensúlyozni a digitális piacokon az aszimmetriát, ami felveti annak lehetőségét, hogy a későbbiekben a végrehajtási problémákat reformokkal kell majd megoldani, éppen úgy, ahogyan a fogyasztóvédelemben a decentralizált végrehajtás problémái a nagy online szolgáltatók esetében a központosított végrehajtáshoz (DSA) vezettek el.

IV. FEJEZET: AZ ELEKTRONIKUS HÍRKÖZLÉSI ADATVÉDELMI IRÁNYELV ÁLTAL BIZTOSÍTOTT VÉDELEM SZINTJE ÉS AZ UTÓBBI ÉVEK JOGALKOTÁSI JAVASLATAI

Az e-Privacy rendelettervezet visszavonása miatt jelenleg az elektronikus hírközlési adatvédelmi irányelv szabályozza a hírközlési szolgáltatásokkal kapcsolatos, különösen az elektronikus kommunikáció során keletkező adatok kezelését, felhasználását és védelmét. Míg a GDPR keretrendelet, vagyis a személyes adatok kezelését általános értelemben szabályozza, addig az elektronikus hírközlési adatvédelmi irányelv egy szektor, egy ágazat szabályait öleli föl, tehát speciális jogszabályként a GDPR rendelkezéseit részletezi és kiegészíti.

E fejezet célja az, hogy a dolgozat alapkoncepciójához illeszkedő és a személyes adatok kezelésével összefüggő szabályozás teljes körű értelmezéséhez hozzájáruljon, ezáltal rámutatva azokra a rendelkezésekre, amelyek képesek az adatvezérelt vállalatok működéséhez közelebb vinni, és átlátni az üzleti modelljeik jogszabályi kereteit. Hangsúlyos kérdés az említett irányelv és a GDPR kapcsolódó pontjainak értelmezése, de érintem a visszavont e-Privacy rendelet tervezetét, valamint a jelenleg javaslat formában létező digitális omnibusz csomagot is. Ez utóbbi kapcsán számbaveszem azokat a tervezett rendelkezéseket, amelyek összefüggenek az elektronikus hírközlési adatvédelmi irányelvvel, és kitérek arra, hogy a csomag milyen hatást gyakorolhat az üzletszerzési célú tájékoztatásokra.

1. Az elektronikus hírközlési adatvédelmi irányelv és a GDPR

A hírközlési ágazatban az alapvető jogok és szabadságok védelmével kapcsolatos területekre vonatkozóan két kiindulási pont azonosítható. Egyrészt alapvetően az elektronikus hírközlési adatvédelmi irányelv rendelkezéseit kell alkalmazni, de azon területek esetében, amelyeket ez az irányelv nem kifejezetten szabályoz, a GDPR-t kell alkalmazni.⁵³⁰ Másrészt a GDPR-t kell alkalmazni „minden olyan esetben, amelyekre nem vonatkoznak azonos célú, az elektronikus hírközlési adatvédelmi irányelvben meghatározott különös kötelezettségek.”⁵³¹

Annak eldöntéséhez, hogy mik azok a különös kötelezettségek, amiket az irányelv nem szabályoz, a GDPR ad segítséget: „A természetes személyek összefüggésbe hozhatók az általuk használt készülékek, alkalmazások, eszközök és protokollok által rendelkezésre bocsátott online azonosítókkal, például IP-címekkel és cookie-azonosítókkal,” ami által „olyan nyomok keletkezhetnek, amelyek [...] egyéb információkkal összekapcsolva felhasználhatók a

⁵³⁰ Elektronikus hírközlési adatvédelmi irányelv (10) preambulumbekzdés

⁵³¹ GDPR (173) preambulumbekzdés

természetes személyek profiljának létrehozására és az adott személy azonosítására.”⁵³² A másik irányból közelítve, de ugyanezt erősíti meg az EDPB vonatkozó iránymutatása: A GDPR „saját tárgyi hatályának (a személyes adat fogalmának) egyértelműsítése során kifejezetten említést tesz olyan adatkezelési tevékenységekről, amelyek – legalábbis részben – az elektronikus hírközlési adatvédelmi irányelv tárgyi hatálya alá is tartoznak.”⁵³³ Ez azt jelenti, hogy a cookie-k tekintetében egyrészt releváns az elektronikus hírközlési adatvédelmi irányelv, és – mivel személyes adatnak is minősülhetnek – releváns a GDPR is.

A cookie-k a felhasználó eszközén tárolt, adott webhelytől származó, kis terjedelmű, szöveges információk. Különböző típusokba sorolják őket, attól függően, hogy mire szolgálnak: egy részük a weboldal használatához, a felhasználói élmény érdekében feltétlenül szükséges; másik részüknek a személyre szabott tartalom kínálásában van szerepe, és gyakran harmadik felektől származnak. Előbbiek körébe tartozik például az, hogy a honlap megjegyzi a látogatásomat, vagy hogy vásárlói kosárban gyűjtöm a kiválasztott árucikkeket. Ha ezeket törvényes célra szánják, használatuk azzal a feltétellel engedélyezhető, hogy „a felhasználók a cookie-k, ill. hasonló eszközök céljáról egyértelmű és pontos tájékoztatást kapnak, annak érdekében, hogy tudomásuk legyen az általuk használt végberendezésen elhelyezett adatokról.”⁵³⁴ Ezt bővíti a rendelkező rész: csak azzal a feltétellel legyen megengedett, ha a felhasználó egyértelmű és teljes körű tájékoztatás alapján ehhez előzetes hozzájárulását adta,”⁵³⁵ ugyanakkor biztosítani kell, hogy a felhasználó a cookie-k tárolását elutasíthassa.⁵³⁶ Ez a rendelkezés nem akadályozza azonban az olyan műszaki tárolást és hozzáférést, amely megfelel a következő két kritérium egyikének: vagy magának a közlésnek a továbbításához szükséges a cookie; vagy olyan cookie, amelyre a felhasználó által kifejezetten kért, az információs társadalommal összefüggő szolgáltatás nyújtásához a szolgáltatónak feltétlenül szüksége van.⁵³⁷ Összegezve tehát a szükséges cookie-kkal kapcsolatban tájékoztatást kell nyújtani, utána beleegyezést kell kérni, de beleegyezés nélkül is elhelyezhetők, ebből pedig az következik, hogy ezek a feltétlenül szükséges cookie-k a tájékozott beleegyezés követelménye alól akár mentesülhetnek is.

⁵³² GDPR (30) preambulumbekkezdés

⁵³³ EDPB: 5/2019. számú vélemény az elektronikus hírközlési adatvédelmi irányelv és az általános adatvédelmi rendelet közötti kölcsönhatásról, különösen az adatvédelmi hatóságok illetékessége, feladatai és hatásköre tekintetében. 33. pont

⁵³⁴ Elektronikus hírközlési adatvédelmi irányelv (25) preambulumbekkezdés

⁵³⁵ Elektronikus hírközlési adatvédelmi irányelv 5. cikk (3) bekezdés

⁵³⁶ Elektronikus hírközlési adatvédelmi irányelv (25) preambulumbekkezdés

⁵³⁷ Elektronikus hírközlési adatvédelmi irányelv 5. cikk (3) bekezdés

A tagállamok – az elektronikus hírközlési adatvédelmi irányelv rendelkezéseinek átültetése során – többféle álláspontot érvényesítenek a cookie-kkal kapcsolatban.⁵³⁸ Magyarországon „csak az érintett felhasználó vagy előfizető világos és teljes körű – az adatkezelés céljára is kiterjedő – tájékoztatását követő hozzájárulása alapján lehet adatot tárolni” a végberendezésén, vagy „az ott tárolt adathoz hozzáférni.”⁵³⁹ A NAIH álláspontja szerint a kizárólag a honlapok működéséhez elengedhetetlenül szükséges cookie-k hozzájárulás alapján nem kezelhetők, hiszen mindenképpen elhelyezésre kerülnek a végfelhasználó eszközén, a megfelelő jogalap a jogos érdek, de tájékoztatás nyújtása ebben az esetben is kötelező; ahol azonban e cookie-k nélkül is használható a honlap, ott a hozzájárulás is elfogadható.⁵⁴⁰

A gyakorlatban gyakran találkozunk szalagon futó információkkal, ún. bannerekkel, amelyek tájékoztatnak a cookie-használatról, egyúttal három lehetőséget kínálnak és linket a részletes tájékoztatóhoz; valamint azzal a megoldással, hogy a felugró ablakban az „összes süti elfogadása” gomb jelenik meg, és a további lehetőségekre csak utalás történik. Ez azonban befolyásolja a felhasználót, kikényszeríti a beleegyezését, ezáltal az ún. sötét megoldások közé tartozik. Mivel „a konfigurációs beállítások felkínálása önmagában nem teljesíti az adatvédelmi (és ePrivacy) követelményeket,”⁵⁴¹ mindenképpen szükséges az elutasítási lehetőséget jelölő gomb megjelenítése is.

Az eltérő tagállami implementáció problémáját tárta fel az EUB, amikor előzetes döntéshozatali kérelemre vizsgálta a Planet49 GmbH nyereményjátékával összefüggésben az általa továbbított személyes adatok kezeléséhez, valamint a résztvevők végberendezésében az információk tárolásához és az ahhoz való hozzáféréshez a felhasználói hozzájárulás kérdéseit. A Planet a személyes adatok kezelésére vonatkozóan üres jelölőnégyzettel kérte a regisztrálók beleegyezését, a cookie-k telepítéséhez és a felhasználói viselkedésnek egy elemző cég általi követéséhez előre beikszelt jelölőnégyzetet használt. Az EUB megállapította, hogy a hozzájárulásnak akkor is aktív magatartáson kell alapulnia, ha a cookie nem tárol személyes adatot (bár jelen ügyben a regisztráció során kért adatok és a kapott regisztrációs szám társítása a cookie-k segítségével tárolt adatokat személyessé teszi), valamint a tárolás időtartamáról, az ahhoz való hozzáférésről is tájékoztatást kell adni a felhasználóknak.⁵⁴² E döntés – az önkéntes,

⁵³⁸ BOROS Anita: *A web-sütik használatának adatvédelmi kérdései*. Pro Futuro 2020/3. 49–50.

⁵³⁹ 2003. évi C. törvény az elektronikus hírközlésről (Eht.) 155. § (4) bekezdés

⁵⁴⁰ NAIH/2018/3567/2/V. 5.

⁵⁴¹ BERCZKI Tamás: *Sütihelyzet Franciaországban – Változóban a „cookie wall” szabályozói megítélése?* Blogbejegyzés. 2021. 04. 05. <https://www.dataprivacy.hu/?p=1899> (letöltés: 2022. 02. 23.)

⁵⁴² ECLI:EU:C:2019:801. A Bíróság ítélete (nagytanács) a C-673/17. sz. ügyben (Cookie-k, előre bejelölt négyzettel megadott hozzájárulás), 2019. október 1.

aktív és tájékozott beleegyezés biztosítása érdekében – kijelölte az irányt a tagállamok számára a nemzeti jogszabályuk felülvizsgálatára vonatkozóan, vagyis az EUB-ítélet hozzájárult az elektronikus hírközlési adatvédelmi irányelv egységes alkalmazásához.

2. Szabályozási terv rendelettel

A hatályos elektronikus hírközlési adatvédelmi irányelvet a „technológiai robbanás fogyasztói korszakának beköszönte előtt,”⁵⁴³ még 2002-ben fogadták el, hét év múlva vizsgálták felül, és módosították is.⁵⁴⁴ Rendelkezett a cookie-kat érintő tájékoztatási kötelezettségről a felhasználók felé, akik dönthetnek arról, hogy beleegyeznek ezek használatába, vagy sem; ezért gyakran cookie- (süti)törvényként aposztrofálják. 2015-ben újra felülvizsgálták,⁵⁴⁵ és egy évvel később, amikor a Bizottság a nagy kapacitású internethálózatok elérhetővé tételének és használatának biztosítását szorgalmazta,⁵⁴⁶ jogalkotási javaslatokat fogalmazott meg a hírközlési szolgáltatások keretszabályozásának reformjára, amely érintette az ennek részét képező elektronikus hírközlési adatvédelmi irányelvet is.

2017-re elkészült az új jogszabály, az e-Privacy rendelet tervezete, az Európai Bizottság elfogadta és közzétette. Felmerül a kérdés: miért szükséges új jogszabály alkotása, miért nem elegendő az elektronikus hírközlési adatvédelmi irányelv módosítása. Bár az Európai Bizottság által készítettett hatásvizsgálat szerint az irányelv céljai – az alapvető jogok tiszteletben tartása, a magán- és a családi élet tiszteletben tartása, a személyes adatok védelme – „továbbra is érvényesek,” három fő problémakört mégis azonosítottak: „a polgárok magánélete az online kommunikáció során nem részesül kellő és hatékony védelemben; a polgárok nem részesülnek hatékony védelemben a nem kívánt, üzletszerzési célú tájékoztatással szemben; a vállalkozások elé akadályt gördítenek a tagállamok egymástól elkülönülő jogszabályai és eltérő jogértelmezése, valamint a nem egyértelmű és elavult rendelkezések.”⁵⁴⁷

⁵⁴³ FÉZER i. m. 55.

⁵⁴⁴ Az Európai Parlament és a Tanács 2009/136/EK irányelve (2009. november 25.) az egyetemes szolgáltatásról, valamint az elektronikus hírközlő hálózatokhoz és elektronikus hírközlési szolgáltatásokhoz kapcsolódó felhasználói jogokról szóló 2002/22/EK irányelv, az elektronikus hírközlési ágazatban a személyes adatok kezeléséről, feldolgozásáról és a magánélet védelméről szóló 2002/58/EK irányelv és a fogyasztóvédelmi jogszabályok alkalmazásáért felelős nemzeti hatóságok közötti együttműködésről szóló 2006/2004/EK rendelet módosításáról

⁵⁴⁵ COM(2015) 192 végleges. A Bizottság közleménye az Európai Parlamentnek, a Tanácsnak, az Európai Gazdasági és Szociális Bizottságnak és a Régiók Bizottságának: Európai digitális egységes piaci stratégia 3.4. pont. Brüsszel, 2015. 05. 06.

⁵⁴⁶ COM(2016) 587 végleges. A Bizottság közleménye az Európai Parlamentnek, a Tanácsnak, az Európai Gazdasági és Szociális Bizottságnak és a Régiók Bizottságának: Az összekapcsoltság a versenyképes digitális egységes piac szolgáltatában: Úton a gigabit alapú európai információs társadalom felé. Brüsszel, 2016. 09. 14.

⁵⁴⁷ SWD(2017) 4 final. Bizottsági szolgálati munkadokumentum: a hatásvizsgálat vezetői összefoglalója, amely a következő dokumentumot kíséri: Javaslat – Az Európai Parlament és a Tanács rendelete az elektronikus hírközlés

Mit jelentenek ezek a felhasználók és a gazdaság oldaláról? A gyorsuló ütemű technológiai fejlődés olyan kommunikációs csatornákat teremtett, amelyek az elektronikus hírközlési adatvédelmi irányelv megalkotása és módosítása idején még nem léteztek. Az újraszabályozás fontos eleme volt az is, hogy rendelettervezet készült az irányelv helyett. Érvként hozható fel a rendelet mellett, hogy a GDPR is rendelet, ehhez az új jogszabálynak lex specialisként kell viszonyulnia, amely pontosítja és kiegészíti a GDPR-t a személyes adatnak minősülő elektronikus hírközlési adatok vonatkozásában.

Az e-Privacy rendelet tervezetével kapcsolatos viták, nézőpontok és véleménykülönbségek közel nyolc év alatt sem rendeződtek, aminek gyökere a jogos érdekekkel, a cookie-kkal kapcsolatos szabályozás volt. A jogos érdek és ezzel együtt a cookie-k kérdése megosztó jellegű terület, „olyan vitális gazdasági érdekeket érint,” hogy az e-Privacy rendelet végleges változata elfogadásának egyik meghatározó gátjává vált.⁵⁴⁸ A véleménykülönbségek elvezettek a tervezet visszavonásához, a bizottsági indoklás szerint „a társjogalkotók várhatóan nem jutnak megállapodásra. Ezenkívül a javaslat elavult, tekintettel néhány közelmúltbeli jogszabályra mind a technológiai, mind a jogalkotási környezetet érintően.”⁵⁴⁹ Utalás ez a Draghi-jelentésre, amely az EU versenyképességének javítása érdekében stratégiai célokat és ajánlásokat fogalmazott meg;⁵⁵⁰ valamint a mesterséges intelligenciával kapcsolatos fejleményekre és a kapcsolódó jogalkotási aktusokra.

3. A digitális omnibusz csomag javaslatának vonatkozó rendelkezései

A megoldáskeresés vezérfonala az egyszerűsítés és a versenyképesség ösztönzése volt. Ennek jegyében született a digitális omnibusz csomag javaslata, amely az első lépés az EU digitális szabálykönyvének, azaz digitális jogszabályai egészének optimalizálása irányában. A szabálykönyv egységes rendszerként kívánja kezelni a digitális technológiákat, a kiberbiztonságot, az online platformokat, a digitális adatokkal kapcsolatos kérdéseket és az elektronikus kommunikációt.⁵⁵¹ Az utóbbi tekintetében ez azt jelenti, hogy a közlések titkosságának védelmét továbbra is az elektronikus hírközlési adatvédelmi irányelv látja el, de ennek szabályozási köréből kiemeli a jogalkotó a személyes adatokra vonatkozó

során a magánélet tiszteletben tartásáról és a személyes adatok védelméről, valamint a 2002/58/EK irányelv hatályon kívül helyezéséről (elektronikus hírközlési adatvédelmi rendelet)

⁵⁴⁸ FÉZER *i. m.* 57.

⁵⁴⁹ COM(2025) 45 final. Mellékletek 28.

⁵⁵⁰ Draghi-jelentés A, Draghi-jelentés B

⁵⁵¹ Digitális omnibusz csomag javaslata: Indoklás 1. pont

rendelkezéseket, tehát a cookie-kra és hasonló nyomkövetési technológiákra vonatkozó szabályokat a GDPR hatálya alá vonja.

A jelenleg hatályos elektronikus hírközlési adatvédelmi irányelv a végberendezéshez való hozzáférést (cookie-k), a GDPR pedig a személyes adatok kezelését szabályozza. A digitális omnibusz csomag javaslata alapján a GDPR-ba illesztendő 88a. cikk összekapcsolja a hozzáférést és az adatkezelést, melynek az az előnye, hogy megszünteti a cookie-kra vonatkozóan a párhuzamos hozzájárulás-kérést, ezért a fogyasztó szempontjából kedvező. A 88a. cikk a természetes személy végberendezésében történő személyesadat-tárolást vagy a már ott tárolt személyes adatokhoz való hozzáférést főszabályként hozzájáruláshoz köti, és csak korlátozott célból, szigorúan szükséges esetekben teszi lehetővé a kezelést hozzájárulás nélkül. Idetartozik az elektronikus hírközlő hálózaton keresztül történő közléstovábbítás; az érintett által kifejezetten kért szolgáltatás nyújtása; összesített információk létrehozása a közönségmérési adatokról (belső használatra); a szolgáltatás vagy a végberendezés biztonságának fenntartása vagy helyreállítása (az érintett által kért szolgáltatáshoz kapcsolódva).⁵⁵² Ezek közül a közléstovábbítás és a kifejezetten kért szolgáltatás az elektronikus hírközlési adatvédelmi irányelvben is benne van, a közönségmérést és a biztonságot egyértelműen nevesíti a digitális omnibusz csomag javaslata. Utóbbi kettő „alacsony kockázatot” jelent az érintettek jogaira és szabadságaira nézve, ezt fogja egyértelműsíteni a Bizottság által ígért korlátozó jegyzék, amely fehérlistaként fog szolgálni azokra az esetekre vonatkozóan, amikor az adatkezelő hozzájárulás nélkül, következképpen jogos érdek alapján kezelheti a személyes adatokat.⁵⁵³ Mivel tervek szerint a 88a. cikk a GDPR-ba épül be; a hozzájárulás e rendeletben már lefektetett szabályaival és a DSA interfész kialakításra vonatkozó rendelkezéseivel együtt tovább erősíti az érintettek és a fogyasztók védelmét, újabb bizonyítékát adva az uniós jogalkotó fogyasztóvédő szemléletének. Ezzel szemben annak is megvan a kockázata, hogy a végberendezések által lehetővé válik a természetes személy adataihoz való hozzáférés, a személy megfigyelése.

A jelenleg hatályos szabályozásban a nyomkövető technológiákkal kapcsolatos gyakori hozzájárulás-kérés és ennek megadása – időigényes, ezért előfordulhat, hogy a végfelhasználó nem olvassa végig a tájékoztatást – a beleegyezés által nyújtott védelmet áthatja alá. Ennek a beleegyezés-fáradtságnak a kiküszöbölésére előremutató lehetőséget fogalmazott meg már az e-Privacy rendelet tervezete is, mely szerint a végfelhasználó megteheti, hogy a szoftverbeállítások révén egy adott szolgáltató részére egy vagy több konkrét célhoz ad

⁵⁵² Digitális omnibusz csomag javaslata 3. cikk 15. pont: 88a. cikk (3) bekezdés

⁵⁵³ Digitális omnibusz csomag javaslata (44) preambulumbekkezdés

hozzájárulást, vagy bizonyos típusú cookie-t engedélyezhet több szolgáltató számára. Megoldásként merült fel az is, hogy a szolgáltatók a szoftverbe illesztenek olyan beállításokat, amelyek lehetővé teszik a végfelhasználók számára a hozzájárulás kezelését engedélyezőlisták felállításával és módosításával, és a felhasználó bármikor vissza is vonhatja a beleegyezését. Ez esetben nemcsak dönthetett volna a felhasználó, hogy kinek/minek a részére és milyen célból adja a hozzájárulását, de segítséget kapott volna ezek kezeléséhez is.⁵⁵⁴ Szintén központosított és érintettet támogató megoldást tartalmaz a digitális omnibusz csomag javaslata: ha a természetes személy végberendezésében történő személyesadat-tárolás vagy a már ott tárolt adatokhoz való hozzáférés megszerzése hozzájáruláson alapul, akkor az adatkezelők online interfészeik segítségével biztosítják az érintettek számára, hogy automatizált és géppel olvasható eszközökkel hozzájárulásukat adják, vagy elutasítsák a hozzájárulás iránti kérelmet (egykattintásos lehetőség), vagy gyakorolják a tiltakozáshoz való jogot; és az adatkezelőknek tiszteletben kell tartani e jelzéseket. A javaslat értelmében a webböngésző-szolgáltatóknak is biztosítaniuk kell a fentiekhez a technikai feltételeket. A géppel olvasható jelzésekre vonatkozóan a Bizottság európai szabványügyi szervezet segítségét is igénybe kívánja venni.⁵⁵⁵

Mindkét megoldás kezelte volna/kezelni kívánja a beleegyezés-fáradtságot; de az érintett szempontjából – véleményem szerint – a digitális omnibusz csomag javaslata praktikusabb, mert beépített, automatizált eszközökkel valósul meg. Ugyanakkor ez a javaslat jelenlegi formájában kevésbé erős védelmet biztosít, mint az e-Privacy rendelet tervezetée, elsősorban a hozzájárulás alóli kivételek nagy száma és azok bizonytalan tartalma miatt, valamint az automatizálás miatt. A tényleges védelmi szintet befolyásolja majd a jogérvényesítés hatékonysága (betartják-e, kikényszeríthető-e) és a technikai megvalósítás minősége; nem beszélve arról, hogy a jelenlegi javaslatot valószínűleg viták és módosítások fogják kísérni, valamint a piacra kész műszaki szabványok előállítása is sok időbe telik.

A cookie-kkal kapcsolatban fontos kérdés a cookie-falak szabályozása. A szolgáltatók részéről jelenleg gyakori megoldás a cookie-k vagy hasonló azonosítók elfogadására kényszerítő cookie-, más szóval sütifal alkalmazása. Úgy működik, hogy ha a felhasználó megtagadja a cookie-kkal kapcsolatos hozzájárulást, akkor a fal technikai eszközökkel korlátozza vagy kizárja a hozzáférést adott weboldalhoz, a felhasználónak tehát két lehetősége marad: vagy lemond az oldal használatáról, vagy elfogadja a cookie-kat. Az elektronikus hírközlési adatvédelmi irányelv esetében a GDPR érvényes hozzájárulásra vonatkozó feltételeit kell figyelembe venni, ebben az esetben ezek egyik eleme, az önkéntesség sérül, ebből

⁵⁵⁴ E-Privacy rendelet tervezete (6087/21) (20a) preambulumbekkezdés

⁵⁵⁵ Digitális omnibusz csomag javaslata 3. cikk 15. pont: 88b. cikk

következően az érintett felhasználónak nincs valódi választási lehetősége, tehát hozzájárulása sem minősül önkéntesnek. Az EDPB ezzel kapcsolatos iránymutatása tiltja a cookie-falak alkalmazását,⁵⁵⁶ s ezt a határozott tiltást hiányolta az e-Privacy rendelet tervezetéből is, ezért nyilatkozatában arra is felhívta a figyelmet, hogy „bele kell foglalni egy, ezt a tilalmat rögzítő külön rendelkezést.”⁵⁵⁷ Idetartozó kérdés az is, hogy mivel a cookie-falak alkalmazása nyomást, befolyást gyakorol a felhasználóra, az ún. sötét megoldások közé tartozik. A digitális omnibusz csomag javaslatában nem szerepel a cookie-falak kifejezett tiltása, de levezethető az EDPB iránymutatásából és a GDPR hozzájárulási feltételeiből.⁵⁵⁸ Úgy vélem, a cookie-falak alkalmazására vonatkozó kifejezett tilalom egységes, közvetlenül alkalmazandó rendelkezést jelentett volna, hozzájárulva a csomag egyszerűsítési és harmonizációs törekvéseihez is.

4. A digitális omnibusz csomag javaslatának hatása a közvetlen üzletszerzési célú tájékoztatás lehetőségére

A közvetlen üzletszerzési célú tájékoztatások gyakorlatát jelenleg a GDPR és az elektronikus hírközlési adatvédelmi irányelv határozza meg. A digitális omnibusz csomag javaslata két tekintetben befolyásolhatja ezt a gyakorlatot: egyrészt a személyes adat fogalmának meghatározásával, másrészt azzal, hogy tartalmaz-e konkrét rendelkezést a közvetlen üzletszerzési célú üzenetekre vonatkozóan.

A csomag a GDPR-hoz képest szűkebben értelmezi a személyes adat fogalmát, amikor hozzáteszi annak definíciójához, hogy „egy természetes személyre vonatkozó információ nem feltétlenül személyes adat minden más személy vagy szervezet számára pusztán azért, mert egy másik szervezet azonosítani tudja az adott természetes személyt.”⁵⁵⁹ Eszerint nem az azonosíthatóságra való képesség a mérvadó, hanem az, hogy egy adott szervezet tudja-e azonosítani a számára rendelkezésre álló eszközökkel, vagy sem; következésképpen a személyes adat fogalma mozgó dimenzióba kerül: ugyanaz az adat egyik vállalat számára személyes adat, a másik számára nem az.

Az álnevesített adatokra vonatkozóan ez azt jelenti, hogy míg a GDPR szerint a természetes személy azonosíthatóságához figyelembe kell venni minden olyan eszközt, amelyet az adatkezelő valószínűsíthetően felhasználhat, addig a javaslat szerint, ha az adott szervezet nem rendelkezik olyan eszközökkel, amelyekkel valószínűsíthetően képes azonosítani a

⁵⁵⁶ EDPB: 5/2020. 13.

⁵⁵⁷ EDPB: 03/2021. nyilatkozat az elektronikus hírközlési adatvédelmi rendeletről. 3.

⁵⁵⁸ GDPR 7. cikk (4) bekezdés

⁵⁵⁹ Digitális omnibusz csomag javaslata 3. cikk 1. a) pont

természetes személyt, akkor az álnevesített adat nem személyes adat. E definíció szubjektív, hiszen az azonosíthatóság az adatkezelőn áll vagy bukik. Ha az álnevesített adat nem személyes adat, akkor nem tartozik a GDPR hatálya alá sem.

Tovább gondolva, a digitális omnibusz csomag javaslatának definíciója hátráltatná a felügyeleti hatóságok munkáját, hiszen minden egyes eset egyedi tényfeltárást kívánna, jogi bizonytalanságot okozhat az érintett szereplők számára, ami ellentétes az omnibusz csomag saját céljával, az egyszerűsítési törekvéssel, valamint ellentétes a Chartával⁵⁶⁰ is. Ugyanakkor az adatvédelem európai vívmányait is fenyegeti, hiszen kikaput jelenthet a tisztességtelen szereplők számára. A javaslatban szereplő végrehajtási jogi aktus meghatározná, hogy mi nem minősül személyes adatnak,⁵⁶¹ ezáltal bizonyos álnevesített adatok kikerülnének a GDPR hatálya alól. Az említett jogi aktus „közvetve jelentős szerepet biztosítana a Bizottságnak abban, hogy teljes iparágakat vonjon ki a GDPR hatálya alól.”⁵⁶² A vonatkozó szakirodalom szerint a fő hasznélvezők valószínűleg nem a kkv-k lesznek – holott a csomag és a digitális szabálykönyv is versenyélénkítő célú –, hanem a nagy technológiai vállalatok, a nyomkövető cégek és az adatbrókerek, aminek hátterében az erőteljes lobbitevékenység azonosítható.⁵⁶³

A közvetlen üzletszerzési célú tájékoztatásokhoz való adatgyűjtéshez, a felhasználói viselkedés követéséhez a szolgáltatók gyakran használnak cookie-kat és egyéb nyomkövető technológiákat, ezek az elektronikus hírközlési adatvédelmi irányelv hatálya alá tartoznak. Ez alapján a felhasználónak előzetesen kifejezetten hozzá kell járulnia az eszközén az adattároláshoz és az ahhoz való hozzáféréshez.⁵⁶⁴ Emellett közvetlen üzletszerzési célból főszabályként kizárólag hozzájárulás alapján használhatók az automatizált hívóberendezések, faxberendezések, küldhetők sms-ek, e-mailek.⁵⁶⁵ Ez szigorúbb követelmény, mint a GDPR-é, mert a szolgáltató nem támaszkodhat más jogalapra, például a jogos érdekre. Ez egyben azt is jelenti, hogy az említett irányelv tilalmat fogalmaz meg a kérértlen üzenetekre vonatkozóan, míg a GDPR tervezett 88a. cikke nem tilalmat tartalmaz, hanem a személyes adatokhoz és a végberendezéshez hozzáférés mikéntjét szabályozza. Amennyiben tehát az elektronikus hírközlési adatvédelmi irányelv jelenleg hatályos, szigorú rendelkezése megszűnik a közvetlen üzletszerzési tájékoztatásokra vonatkozóan, és beleolvad a GDPR rugalmasabb

⁵⁶⁰ Charta 8. cikk

⁵⁶¹ Digitális omnibusz csomag javaslata 3. cikk 10. pont (1) bekezdés

⁵⁶² NOYB.EU: *Digital Omnibus Analysis of Select GDPR and ePrivacy Proposals by the European Commission* Version 2.0. 2026. január. 7. <https://noyb.eu/sites/default/files/2025-12/noyb%20Digital%20Omnibus%20Report%20V1.pdf>, letöltés: 2026. 02. 01.

⁵⁶³ NOYB.EU: *Digital Omnibus* 13.

⁵⁶⁴ Elektronikus hírközlési adatvédelmi irányelv 5. cikk (3) bekezdés

⁵⁶⁵ Elektronikus hírközlési adatvédelmi irányelv 13. cikk

jogalaprendszerébe, akkor megnőhet a jogos érdek szerepe, valamint ezzel párhuzamosan az adatvédelem szintje csökkenhet, ami táptalajt nyújthat a közvetlen üzletszerzési célú tájékoztatások áradásának.

5. Összegzés és következtetés

Korunk egyik sürgető kihívása a magánélet védelme a személyes adatok kezelésével összefüggésben, ugyanakkor gazdasági szükségszerűség ezen szabad áramlásának támogatása. E látszólag ellentétes célok összesimulását, harmóniába olvadását az EU adatvédelmi reformja kívánja megvalósítani, amelynek egyik követelménye az, hogy rendelkezései egységesek és naprakészek legyenek. A 2018-tól alkalmazandó GDPR-ral együtt az e-Privacy rendeletnek is életbe kellett volna lépnie, de a tervezetét 2025-ben visszavonták.

Az EU digitális szabálykönyve részeként készült – a verseny élénkítése, a harmonizáció és az egyszerűsítés érdekében – a digitális omnibusz csomag javaslata, amelynek részét képezi a természetes személy végberendezésében történő személyesadat-tárolás vagy a már ott tárolt személyes adatokhoz való hozzáférés szabályozása. A javaslat alapján az elektronikus hírközlési adatvédelmi irányelv cookie-kra vonatkozó szabályozása a GDPR feladata lesz, ennek értelmében a jogalkotó a személyes adatok védelmére vonatkozó rétegeket egységes rendszerbe helyezi. A cookie-kkal kapcsolatban a GDPR-on belül egységesíti a hozzájárulás szabályait, egy kattintással teszi lehetővé az érintetti hozzájárulás megadását vagy az elutasítást, és az alacsony kockázatú cookie-k használatát nem köti hozzájáruláshoz. E javaslat hatással lehet a közvetlen üzletszerzési célú tájékoztatásokra mind a személyes adat fogalmának módosítása által, mind az ilyen üzenetek küldése tekintetében. Előző csökkentheti a személyes adatok körét, kiemelve ezeket a GDPR hatálya alól, ami tágabb lehetőséget ad a vállalatok számára a marketingcélú üzenetek küldésére; utóbbi mint tilalom megszűnhet, ami a GDPR jogalapjainak rugalmasabb alkalmazását teszi lehetővé.

A digitális omnibusz csomag javaslata egy újabb kísérlet arra, hogy az adatvédelem ne álljon útjában az adatok szabad áramlásának, ezáltal gazdaságélénkítő hatása is jelentős legyen. Illeszkedik abba a folyamatba, amivel az EU az adatok gazdasági szerepének támogatása és az adatok védelme egyensúlyát, harmóniáját igyekszik megtalálni. Ugyanakkor a javaslat versenyélénkítő pontjai – a vonatkozó szakirodalom szerint – inkább az adatvezérelt nagy platformoknak kedveznek, azok jogi és technikai kapacitása, valamint merészebb kockáztvállalása miatt, ami nem serkenti az adatoknak a digitális gazdaságban való erőteljesebb felhasználását a kisebb európai vállalkozások esetében, a felhasználó szempontjából pedig tovább erősödik az információs aszimmetria.

V. FEJEZET: A SZEMÉLYES ADATOK ÉS AZ ADATVÉDELEM SZEREPE A PIACI VERSENYT ÉRINTŐ PLATFORMJOGSZABÁLYOKBAN

A személyes adatok alapozták meg az online platformok hatalmát, amelyet először a GDPR rendelkezéseivel, a természetes személyek szempontjából igyekezett az EU fékezni, de úgy, hogy egyúttal ezen adatok szabad áramlását is céljai közé emelte. A platformok a big data kezelésével és a tisztességtelen piaci magatartással olyan erőfölényhez jutottak, amellyel képesek visszaélni, ezért a hagyományos versenyjogi vizsgálatok és az összefonódás-ellenőrzési vizsgálatok tapasztalatai arra késztették az EU-t, hogy célzott rendeletekkel ex ante szabályozza ezeket. Valójában a személyes (és nem személyes) adatok kezelésének platformokra vonatkozó, piaci versenyt érintő szabályozási igénye hívta életre a platformjogszabályokat, amelyeknek számos rendelkezése a GDPR-ból nőtt ki. Jelen fejezet a személyes adatok és az adatvédelem szerepét vizsgálja a platformjogszabályokban, egyúttal elemzi az antitröszt- és a fúziós ügyek folyamatát és hatását e jogszabályokra. Mindezek előtt azonban azt is meg kell vizsgálni, hogy a GDPR rendelkezései hozzájárulnak-e az adatok szabad áramlásához, ezzel együtt elősegítik-e a piaci versenyt.

1. A GDPR mint fékezőerő?

A GDPR megalkotásának hátterében – bár az nem említi az online platform kifejezést⁵⁶⁶ – lényegében a közösségi oldalak, tágabban a platformjelenségek és gazdasági-társadalmi hatásaik álltak. A GDPR egyrészt a természetes személyek alapvető jogait és különösen a személyes adatok védelméhez való jogukat védi,⁵⁶⁷ másrészt a személyes adatok szabad áramlása előtti akadályokat kívánja lebontani az egységes szabályozással.⁵⁶⁸ Előbbi alapjogot véd, utóbbi belső piaci cél, e kettő mégsem kerül konfliktusba, mert a védelem teremti meg a személyes adatok szabad áramlásának lehetőségét és feltételeit. Az adatvédelem és a gazdasági cél azonos jogi keretbe helyezése fokozza az áttekinthetőséget, csökkenti a tagállami széttöröttségét, növeli a jogbiztonságot, ezáltal jótékony hatással bír a gazdasági versenyre is, különösen a digitális piac működésére.

A GDPR azonban tartalmaz olyan szabályszerűségeket, amelyek fékezhetik a versenyképességet és az innovációt. Ilyenek a megfelelés érdekében támasztott követelmények – mint például az adatvédelmi hatásvizsgálat, az elszámoltathatóság –, amelyek költségnövelő

⁵⁶⁶ ZÖDI (2022) i. m. 68.

⁵⁶⁷ GDPR 1. cikk (2) bekezdés

⁵⁶⁸ GDPR 1. cikk (3) bekezdés és (10) preambulumbekkezdés

hatásuk miatt nagy terhet jelentenek a kkv-k számára, csakúgy, mint a kiszabható bírság nagyságrendje, ezáltal a piacralépési esélyeiket is rontva. A személyes adatok szabad áramlását közvetlenül befolyásolja az, hogy a harmadik országokba irányuló adattovábbítások megfelelőségi határozathoz vagy garanciákhoz kötöttek,⁵⁶⁹ ami jogi bizonytalanságot, költségnövekedést és versenyhátrányt jelenthet azokkal a rivális vállalkozásokkal szemben, amelyeknek kevésbé szigorú adatvédelmi rendelkezéseknek kell megfelelni. Az adatkezelés jogszerű jogalapja és elvei, különösen az adattakarékosság és a célhoz kötöttség⁵⁷⁰ főleg a kkv-k gazdasági lehetőségeit korlátozza, hiszen a nagy adatvezérelt vállalkozások bátrabban vállalják be a hatósági vizsgálatokat és következményeit, ismerve és kihasználva a GDPR decentralizált végrehajtásának nehézségeit.

A digitális gazdaságra vonatkozó mutatók kedvezőtlen helyzetről számolnak be. 2019-ben a világ hetven legnagyobb digitális platformjának értékéből az USA és Kína több mint 90%-kal részesedett,⁵⁷¹ s ez az arány később sem javult, az EU részesedése csupán néhány százalék körül van.⁵⁷² Az EU gyenge a növekedést előmozdító technológiák terén, a világ ötven legnagyobb technológiai vállalata közül csak négy európai, és azok sem a fogyasztókkal való interakcióhoz kötöttek.⁵⁷³ A harmadik országokba továbbított uniós adatok mennyisége 90%-ra becsülhető.⁵⁷⁴ Természetesen nem teljes mértékben, de a felsorolt adatok magyarázhatók azzal is, hogy a GDPR-ban az alapjogi védelem hangsúlyosabb, mint az adatok szabad áramlásának támogatása. Ezzel szemben az USA adatvédelmi gondolkodása a piaci viszonyokat, Kínáé az állami kontrollt helyezi előtérbe, de az adatokat mindkettő kevésbé szigorúan védelmezi, ezáltal a digitális szektor növekedését segítik elő. A GDPR hozadékaként az EU szabályozási irányvonalat tudott kialakítani az adatvezérelt nagyvállalatok révén a globális piacon, szabályozási hegemoniáját Brüsszel-hatásnak nevezik, ezt azonban geopolitikai feszültségek terhelik és fenyegetik.⁵⁷⁵ Összegezve az állapítható meg, hogy a GDPR nem járul hozzá Európa globális versenyképességének javításához, az innovációt a szabályozások akadályozzák. A másik oldalon az adatvezérelt platformok folyamatos

⁵⁶⁹ GDPR V. fejezet

⁵⁷⁰ GDPR 6. cikk és 5. cikk (1) bekezdés b) és c) pont

⁵⁷¹ TRUUST.IO: *U.S. and China share the digital economy pie*. <https://truust.io/blog/u-s-and-china-share-the-digital-economy-pie/> (letöltés: 2021. 02. 02.)

⁵⁷² UNCTAD: *2025 Technology and Innovation Report*. 2025. 7. https://unctad.org/system/files/official-document/tir2025_en.pdf (letöltés: 2026. 02. 02.)

⁵⁷³ Draghi-jelentés A. 5.

⁵⁷⁴ Draghi-jelentés B. 67.

⁵⁷⁵ Anu BRADFORD: *The Brussels Effect: How the European Union Rules the World*. 2019, Abstract. <https://doi.org/10.1093/oso/9780190088583.001.0001> (letöltés: 2022. 10. 22.). RÉVÉSZ Béla Ákos: *A Brüsszel-hatás végnapjai*. 2025. december 10. <https://makronom.eu/2025/12/10/brusszel-szabalyozas-big-tech-egyesult-allamok-trump-haboru-makronom-revesz-elemzes/> (letöltés: 2025. 12. 30.)

erősödése figyelhető meg, ami arra enged következtetni, hogy a GDPR intézkedései nem tudják megfelelő mértékben kezelni a digitális piacokon észlelhető problémákat, sőt éppen ellenkezőleg, hozzájárulnak helyzetük erősödéséhez.⁵⁷⁶ Az online platformok szabályozásának folyamatában először a meglévő normák kereteit alkalmazták, majd – Zódi Zsolt megállapítása alapján⁵⁷⁷ – 2019-től datálhatók, és sui generis platformjogként azonosíthatók azok a jogszabályok, amelyeket az EU kifejezetten a platformok szabályozása érdekében alkotott. Az elnevezés alapja az, hogy e jogszabályok a hagyományos jogterületek ismert szabályaiból merítenek, de ugyanakkor alkalmazkodnak a platform logikájához vagy az adott ágazathoz.⁵⁷⁸

A DMA, a DSA és a Data Act tartozik a platformjogszabályok közé, ezekben a személyes adatok fontos szerepet töltenek be, ezáltal kapcsolatot mutatnak a GDPR-ral. Közös céljuk az, hogy hozzájáruljanak a belső piac megfelelő működéséhez, a versengő és tisztességes piac biztosításához. A továbbiakban a felsorolt jogszabályokra fókuszálva (a DSA-val erőteljes fogyasztóvédelmi vonatkozásai miatt a VI. fejezetben foglalkozom) azokat a rendelkezéseket tekintem át, amelyek a személyes adatok felhasználásának piaci versenyt befolyásoló szerepét szabályozzák, ezáltal az adott rendelet és a GDPR érintkezési pontjaira is rávilágítanak.

2. A DMA

A GDPR alkalmazásával kapcsolatos bizonytalanságokra és a közös európai adatvédelmi kultúra hiánya⁵⁷⁹ okozta problémákra reflektál a digitálisjogszabály-csomag egyik rendelete, a DMA, és „az antitröszt fogalomrendszerét kölcsönözve,”⁵⁸⁰ a korábbi versenyügyek tapasztalatait felhasználva előzetesen, ex ante eszközökkel állapít meg kötelezettségeket, és fogalmaz meg közvetlen tiltásokat. A kötelezettségek és a tiltások címzettjei az Európai Bizottság által kapuörnek minősített, alapvető platformszolgáltatást nyújtó, megszilárdult piaci pozíciót birtokló vállalatok, de nem címzettje a digitális piac többi

⁵⁷⁶ GOMBOS Katalin: *A Digital Services Act és a Digital Markets Act várható kihívásai a jogalkalmazásban*. In Medias Res 2023/2. 93–94. A további okokra bővebben rávilágítanak: COM(2024) 357 final; COM(2020) 264 final; EDPB: Contribution of the EDPB to the report on the application of the GDPR under Article 97 Adopted on 12 December 2023. https://www.edpb.europa.eu/system/files/2023-12/edpb_contributiongdprevaluation_20231212_en.pdf (letöltés: 2024. 08. 22.); EDPB: 'Safeguarding individuals' digital rights: EDPB Annual Report 2023, 2024. április 23. [edpb annual report 2023 en.pdf](https://www.edpb.europa.eu/system/files/2024/04/edpb_annual_report_2023_en.pdf) (letöltés: 2024. 05. 23.); 2014/C 225/07. Az európai adatvédelmi biztos előzetes véleményének összefoglalója az adatvédelemről és a versenyképességről az óriás méretű adathalmazok korában; GOMBOS i. m. 105–113.; Wolfgang KERBER – Karsten K. ZOLNA: *The German Facebook case: the law and economics of the relationship between competition and data protection law*. European Journal of Law and Economics 2022/54. 228. <https://doi.org/10.1007/s10657-022-09727-8> (letöltés. 2024. 02. 02.)

⁵⁷⁷ ZÓDI (2022) i. m. 72.

⁵⁷⁸ ZÓDI (2022) i. m. 75.

⁵⁷⁹ COM(2020) 264 final. 2. pont

⁵⁸⁰ FIRNIKSZ Judit: *Pillanatkép a digitális piacok szabályozásáról: A DMA a vállalati compliance tükrében*. Doktori értekezés. Bp., 2023. 33.

szereplője. Ezzel a DMA kiegészíti az EUMSZ 102. cikkében foglaltakat: elismeri a kapuőrök piacvezető pozícióját – „kvalitatív és kvantitatív kijelölési feltételek rendszerével” kikerülve a piac meghatározását⁵⁸¹ –, erőfölényük ellen nem lép fel, csak az ezzel való visszaélést tilalmazza a tisztességes gazdasági verseny érdekében. Azért kapták a kapuőr nevet, mert – mint a hírszerkesztők, akik eldöntik, milyen hírek jutnak el az olvasókhoz – őrizték a „kaput,” megakadályozva, hogy a feltörekvő digitális vállalkozások piacra lépjenek, és hogy kinyíljon a kapu a verseny előtt az alapvető platformszolgáltatások⁵⁸² nyújtásának piacán. Azért találó az elnevezés, mert utal arra, hogy a DMA kezükbe adja a tisztességes magatartáshoz és versenyhez vezető út kulcsát, s ezzel megnyílhat a kapu a verseny, a fogyasztók digitális jóléte felé.

A GDPR és a DMA célmeghatározása más-más oldalról közelít a középponti szerepű személyes adatokhoz (fogalmát a DMA a GDPR definíciójára utalással adja meg⁵⁸³), előbbi a kezelésével összefüggésben a védelmét és a szabad áramlását hangsúlyozza; utóbbiban mint gazdasági input, mint nyersanyag jelenik meg, amely köré (is) épülnek a jól működő digitális piac elvárásai, és fogalmazódnak célelemekké. A DMA kulcsfontosságú célja a versengő és tisztességes piac, amely a belső piac működését és a felhasználókat is szolgálja, ill. hozzájárulhat a személyes adatok GDPR-ban kiemelt szabad áramlásához.⁵⁸⁴ A digitális piac fogalmának meghatározásával azonban adós marad a DMA.

A személyi hatályt illetően a GDPR a természetes személyeket nevezi meg,⁵⁸⁵ a DMA pedig a vég- és az üzleti felhasználók kategóriáját alkalmazza. A végfelhasználó és az üzleti felhasználó fogalmak jelentése a felhasználásjellegét és a gazdasági tevékenységhez kötöttséget emeli ki, másrésztől mindkettő magában hordozza a fogyasztói jogviszonyt is a kapuőrökkel és a platformszolgáltatásokkal összefüggésben,⁵⁸⁶ ami a fogalommeghatározásokban szereplő definíciókból is levezethető.⁵⁸⁷ Jelentős különbség az, hogy a DMA mindkét kategóriába bevonja a természetes személyek mellett a jogi személyeket is; utóbbiakat azért, mert a platformhasználat során hasonlóan kedvezőtlen alkupozícióba⁵⁸⁸ kerülnek, mint a természetes személyek.

⁵⁸¹ FIRNIKSZ *i. m.* 49.

⁵⁸² DMA 2. cikk 2. a)–i) pont alapján az alapvető platformszolgáltatások körébe tartoznak a következők: online közvetítő szolgáltatás; keresőprogram; közösségi hálózati szolgáltatás; videomegosztóplatform-szolgáltatás; számfüggetlen személyközi hírközlési szolgáltatás; operációs rendszer; webböngésző; virtuális asszisztens; felhőszolgáltatás és az online hirdetési szolgáltatás.

⁵⁸³ DMA 2. cikk 25. pont

⁵⁸⁴ GDPR 1. cikk (1) bekezdés

⁵⁸⁵ GDPR 1. cikk (1) bekezdés

⁵⁸⁶ HOHMANN Balázs: *A Digital Services Act és a Digital Markets Act termékekre és digitális szolgáltatásokra irányuló fogyasztói jogviszonyokat érintő rendelkezései*. In *Medias Res* 2023/2. 74.

⁵⁸⁷ DMA 2. cikk 20. és 21. pont

⁵⁸⁸ HOHMANN *i. m.* 74.

2.1. A GDPR és a DMA rendelkezéseinek összevetése a személyes adatok tekintetében

A személyes adatok jogszerű kezeléséhez a GDPR többféle jogalapot ismer el,⁵⁸⁹ ezzel szemben ezek közül a DMA csak egyet, a hozzájárulást: a végfelhasználók dönthetnek a személyes adataik kapuőr általi összekapcsolásának engedélyezéséről, és ugyanez vonatkozik a kapuőr által nyújtott más szolgáltatásból és a harmadik fél által nyújtott szolgáltatásból származó adatokra is.⁵⁹⁰ Ez azt jelenti, hogy a kapuőrök más jogalapra, például a jogos érdekre nem tudnak hivatkozni. Abban az esetben, ha a végfelhasználó úgy dönt, hogy nem engedélyezi adatai kapuőr általi összekapcsolását, kombinálását, akkor az – megfelelő tájékoztatás mellett – kisebb mértékű személyre szabással járó ajánlathoz vezethet; de nem járhat azzal, hogy a kapuőr lerontja az alapvető platformszolgáltatások feltételeit vagy minőségét, vagyis a szolgáltatás változatlan marad.⁵⁹¹ Ez abban a tekintetben előnyös, hogy a kapuőr nem tudja a hozzájárulást kikényszeríteni, tehát kevesebb lehetősége marad a személyes adatok profilalkotáson, algoritmikus megoldásokon alapuló kezelésére. A DMA-vel foglalkozó tanulmányok szerzői elismerik a kapuőrökre rótt kötelezettségek és tiltások értékeit, de aggályaikat is megfogalmazzák azok kikényszeríthetőségét illetően; míg mások szkeptikusabbak.⁵⁹²

A Kerber–Specht–Riemenschneider szerzőpáros tanulmánya azt a szakpolitikai szintű beavatkozási lehetőséget javasolta a DMA-tervezet kapcsán, hogy teljes, közvetlen tilalmat vezessen be a személyes adatoknak a kapuőr általi keresztfelhasználására, összekapcsolására a más szolgáltatásokból és a harmadik fél által nyújtott adatok tekintetében, vagyis hogy ne hagyja meg azt a kikaput a kapuőrök számára, hogy a végfelhasználók hozzájárulása alapján felhasználhassák ezeket az adatokat.⁵⁹³ Ezzel a megoldással jobb versenyfeltételeket, alacsonyabb belépési korlátokat lehetett volna biztosítani a piaci versenyben, valamint meg lehetett volna szüntetni az adatvédelmi kockázatokat és a végfelhasználók vonatkozásában fennálló információs aszimmetriát is. A DMA végleges normaszövege azonban éppen a kiváltó okot nem szüntette meg, csupán korlátozottabb lehetőséget hagyott a kapuőröknek a személyes adatok felhasználását illetően.

⁵⁸⁹ GDPR 6. cikk

⁵⁹⁰ DMA 5. cikk (2) bekezdés

⁵⁹¹ DMA (36)–(37) preambulumbekkezdés és 13. cikk (6) bekezdés

⁵⁹² BAK Márton Ferenc – BORDÁS Péter: *Reguláció – dereguláció: Kihívások és lehetőségek a digitális piacok szabályozásában*. In: GLAVANITS Judit – SZABÓ Tamás (szerk.): *Kiszolgáltatott csoportok a digitális világban: A digitalizáció jogalkotói és jogalkalmazói kihívásai*. Universitas–Győr Nonprofit Kft., 2024. 18.

⁵⁹³ KERBER–SPECHT–RIEMENSCHNEIDER i. m. 75.

Ebben a megoldásban – véleményem szerint – a jogalkotó olyan egyensúlynövelő intézkedéssel válaszolt a platformok gyakorlatára, amellyel minden érintett felet arányosan közelített egymáshoz. A végfelhasználók választhatnak, vagy adják a hozzájárulásukat az említett adatok összekapcsolására, élvezve esetleg a preferenciáiknak megfelelő ajánlatokat, vagy nem adják hozzájárulásukat, és ebben az esetben is változatlanul használhatják az alapvető platformszolgáltatásokat. Az üzleti felhasználók számára tisztességes feltételeket teremtett, ezáltal számtalan olyan előnyhöz jutnak, amely által felzárkóztathatják az európai adatgazdaságot. A kapuőröknek megmaradt a hozzájáruláson alapuló adatkezelés lehetősége. Utóbbi két felet várhatóan innovatív megoldásokra fogja sarkallni a DMA, az üzleti felhasználókat a piacnyitás lehetőségeinek kiaknázására, a kapuőröket a szigorításokat ellensúlyozó megoldásokra.⁵⁹⁴ A jogalkotói szándék tehát védelmet és teret ad a nem kapuőr vállalkozásoknak; de nem védi a végfelhasználókat, hanem – mivel az információs aszimmetria sem szűnik meg – továbbra is rájuk terheli azt a felelősséget,⁵⁹⁵ hogy beleegyeznek-e személyes adataik kezelésébe, vagy sem.

Az adathordozhatósághoz való jog megjelenése a DMA-ben a GDPR-ból eredeztethető, mely szerint az érintett jogosult az adatkezelő rendelkezésére bocsátott személyes adatait megkapni (ha a jogalap hozzájárulás vagy szerződés volt, és az adatkezelés automatikus), továbbá jogosult ezen adatok továbbítására másik adatkezelő részére.⁵⁹⁶ Ez az a pont, ami versenyjogi lehetőséget rejt magában a DMA szabályozását illetően. A 29. cikk szerinti munkacsoport megállapítása szerint az adathordozhatósági jog segíti a személyes adatok szabad áramlását, új szolgáltatások kidolgozását teszi lehetővé.⁵⁹⁷ Ezt a lehetőséget úgy támogatja a DMA, hogy három tekintetben kiterjeszti a GDPR vonatkozó rendelkezéseit. Egyrészt az adathordozhatóság nemcsak a természetes személyekre vonatkozik, hanem a végfelhasználókra és az általuk felhatalmazott harmadik felekre, vagyis az üzleti felhasználókra is, akik/amelyek többnyire jogi személyek. Másrészt a végfelhasználók által az alapvető platformszolgáltatásokkal összefüggésben szolgáltatott vagy annak használata során keletkezett valamennyi adatra vonatkozik, és ezek egy része (főleg a szolgáltatott adatok) személyes adat. Harmadrészt, míg a GDPR a múltban összegyűjtött adatok hordozhatóságát biztosítja, addig a DMA folyamatos és valós idejű, tényleges hordozhatóságot kínál.⁵⁹⁸ Az adathordozhatósághoz

⁵⁹⁴ A szakirodalomban más lehetőség is megfogalmazódik: „nem világos még, hogy a platformműködésre, és ezen belül a kapuőri működésre az innováció gátjaként vagy ugródeszkájaként kell-e a szabályozás oldaláról tekintenünk.” FIRNIKSZ *i. m.* 33.

⁵⁹⁵ WAERDT *i. m.*

⁵⁹⁶ GDPR 20. cikk

⁵⁹⁷ WP242. 3.

⁵⁹⁸ DMA 6. cikk (9) bekezdés

való jog ezen kiegészítésekkel már alkalmas lehet arra, hogy a felhasználók könnyebben váltsanak az online platformok között, esetleg párhuzamosan használják azokat. A másik oldalról, az üzleti felhasználók szempontjából pedig lehetőséget teremt arra, hogy – ismerve a releváns adatokat – alkalmazkodjanak a piaci viszonyokhoz, reagáljanak a felhasználók igényeire. Mindezek hozzájárulhatnak a piac élénkítéséhez, ezáltal a fogyasztók számára is előnyös lehet.

A DMA adathozzáférésre vonatkozó rendelkezése értelmében a kapuőrnek – az online keresőprogramokat nyújtó vállalkozások kérésére – hozzáférést kell biztosítania a kapuőr online keresőprogramjával végzett keresések során a végfelhasználók által generált rangsorolási, keresési, kattintási és megtekintési adatokhoz. Ezek az adatok lehetnek személyes vagy nem személyes adatok, ezért a DMA a személyes adatok védelme érdekében anonimizálási kötelezettséget ír elő.⁵⁹⁹ Az anonimizálás jelentését a DMA lényegében a GDPR-ral azonosan határozza meg.⁶⁰⁰

A platformok és az ökoszisztémák stratégiája az, hogy elzárják az utat a versenytársaktól, ezért a DMA az adathozzáférés és -hordozhatóság tekintetében többször hangsúlyozza az interoperabilitást.⁶⁰¹ Ha azonban az adatokat kiszakítják az eredeti környezetükből (ex-situ adathasználati jog), akkor a nyers adathalmaz üzleti értéke jelentősen csökken.⁶⁰² A megoldáshoz vezető utat maga a DMA jelöli ki: olyan hatáskört ruház a Bizottságra, amelynek része lehet az operatív és technikai szabályok megállapítása vagy műszaki szabványok kidolgozásának szorgalmazása.⁶⁰³ Továbbá – a DMA és a GDPR kölcsönhatásának vizsgálata során – a Bizottság és az EDPB közös iránymutatás-tervezetet készített, melyben kiegészítve a DMA elvárásait (határidők, versenytársak egyenlő hozzáférése, működőképesség) azokra az adatvédelmi előírásokra is fókuszál, amelyeket az interoperabilitás során be kell tartani: jogalap, adatminimalizálás, felhasználói hozzájárulás.⁶⁰⁴

A DMA személyes adatokkal összefüggő rendelkezéseinek jelentősége az, hogy a digitális piac szereplőinek lehetőségei és helyzete jelentősen megváltozik. A végfelhasználók, fogyasztók korábbi kiszolgáltatott, kapuőröktől függő helyzetét nagyobb választék és az innováció okozta előnyök váltják fel; az üzleti felhasználók korábbi függőségét, ezzel együtt a

⁵⁹⁹ DMA 6. cikk (11) bekezdés

⁶⁰⁰ DMA (61) preambulumbekzdés, GDPR (26) preambulumbekzdés

⁶⁰¹ DMA 6. cikk (7) és (9) bekezdés

⁶⁰² BEYER Fülöp: *In situ adathozzáférési jogok*. <https://www.ludovika.hu/blogok/itkiblog/2023/02/23/in-situ-adathozzaferesi-jogok/> (letöltés: 2024. 01. 02.)

⁶⁰³ DMA (99) és (96) preambulumbekzdés

⁶⁰⁴ EUROPEAN COMMISSION – EDPB: *Joint Guidelines on the Interplay between the Digital Markets Act and the General Data Protection Regulation*. 2025. 10. 09. 7. fejezet. https://www.edpb.europa.eu/our-work-tools/documents/public-consultations/2025/joint-guidelines-interplay-between-digital_hu (letöltés: 2025. 11. 12.)

tisztességtelen, kizsákmányoló üzleti környezetet egyenlő versenyfeltételek, a tisztességesebb üzleti környezet váltja fel. Ezek egyúttal azt is jelentik, hogy a versenyjogi szabályozás fogyasztóvédelmi eredményt is hozhat. (Részletezi az 5. melléklet.)

3. A Data Act

Az innováció fontos lépés a gazdaság felpörgetésére, s ehhez az EU további feltételeket teremt az adatok újrafelhasználását lehetővé tévő Data Act megalkotásával. A Data Act abba a folyamatba ágyazódik, amellyel az EU a személyes adatok erőteljes védelmét célzó álláspontot továbbra is megtartva – de felismerve azok piaci versenyben betöltött input szerepét – a minél szélesebb körű adatfelhasználás irányába mozdult el. A Data Act célja, hogy biztosítsa az adatokból származó értéknek az adatgazdaság szereplői közötti méltányos elosztását.⁶⁰⁵

E szereplők között találunk már ismerősöket: például az érintettet és a kapuőrt, valamint újakat: például az adatbirtokost. Közülük az érintett és vele összefüggésben a személyes adat fogalmát a GDPR-ra utalva határozza meg a Data Act, a kapuőr fogalmát a DMA-re utalva, és a nem személyes adat fogalmát nem utalással, de lényegében a DMA szerint definiálja. A Data Act fogalomhasználatában az adatbirtokos természetes vagy jogi személy, akinek/amelynek joga vagy kötelezettsége olyan adatokat – többek között termékadatokat vagy kapcsolódószolgáltatás-adatokat – használni és rendelkezésre bocsátani, amelyeket a kapcsolódó szolgáltatás nyújtása során visszanyert vagy generált;⁶⁰⁶ tehát jellemzően a gyártót jelenti. A Data Act szerinti felhasználó szintén természetes vagy jogi személy, általában az összekapcsolt termék tulajdonosa, vagy akire/amelyre szerződésben ideiglenes jogokat ruháztak át az adott termék használatára vonatkozóan, vagy aki/amely kapcsolódó szolgáltatást vesz igénybe.⁶⁰⁷

A Data Act hatálya alá tartoznak azon összekapcsolt termékek – IoT-termékek –, amelyek a teljesítményükre, a felhasználásukra vagy a környezetükre vonatkozó adatokat szereznek meg vagy generálnak, és amelyek képesek az említett adatokat kommunikálni.⁶⁰⁸ Ilyen termékek a csatlakoztatott autók, az okosotthon eszközei (mosógép, robotporszívó, kazán, légkondicionáló berendezés), de akár a repülőgépek, a mezőgazdasági gépek is. Ezekhez online szolgáltatások kapcsolódnak, például a mosógépre telepített szolgáltatás nemcsak annak távolról történő bekapcsolását szolgálja, hanem képes mérni a mosással összefüggő

⁶⁰⁵ Data Act (119) preambulumbekkezdés

⁶⁰⁶ Data Act 2. cikk 13. pont

⁶⁰⁷ Data Act 2. cikk 12. pont

⁶⁰⁸ Data Act (14) preambulumbekkezdés

paramétereket (ruha tömege, mosószer mennyisége stb.), és ezek alapján állítja be a mosási ciklust. A termelt adatok – amennyiben megosztásra kerülnek – forrásai lehetnek további szolgáltatásoknak. Ennek egyszerű példája az, hogy az autók által összegyűjtött adatokhoz ne csak a gyártók és a velük szerződött szervizek férjenek hozzá, hanem az adatok megosztása által más szerviz vagy akár a biztosítótársaságok is. Mindez gazdaságélénkítő hatással bír, és ezzel párhuzamosan a fogyasztók alacsonyabb árakra számíthatnak.

Az IoT-termékek által termelt adatok vagy a termék beépített adattárából, vagy a továbbított adatokat fogadó távoli szerverről érhetők el, amely lehet a gyártóé, egy harmadik félé vagy valamely felhőszolgáltatóé.⁶⁰⁹ A Data Act – erősítendő az európai felhőszolgáltatókat, amelyek az amerikai és kínai székhelyűekhez képest elenyésző részesedéssel bírnak⁶¹⁰ – lehetővé teszi a felhasználók számára a felhőszolgáltató-váltást. Ez azért fontos, mert mind a gazdasági ágazatokat, mind a háztartásokat egyre erőteljesebben uralják az IoT-termékek, és a generált adatok tetemes része a számítási felhőbe kerül.

Amennyire teljes és komplex a GDPR a személyes adatok kezelésével kapcsolatban, annyira az a Data Act az adatmegosztásra vonatkozóan, s még inkább így lesz ez a digitális omnibusz csomag javaslata szerint. Elfogadása után a Data Act öleli majd föl az adatok gazdasági értékének kiaknázását elősegítő szabályozást,⁶¹¹ szabad utat engedve az innovatív felhasználásnak.

3.1. A GDPR és a Data Act rendelkezéseinek összevetése a személyes adatok tekintetében

A felhasználók hozzáférését az általuk generált adatokhoz és az adatmegosztás hatókörét a Data Act II. fejezete szabályozza. A 2026. szeptember 12. után forgalomba hozandó IoT-termékek és a kapcsolódó szolgáltatások esetében alapvető követelmény lesz a tervezés, a gyártás és a szolgáltatások nyújtása során, hogy az adatok, ideértve a metaadatokat is – alapértelmezés szerint – közvetlenül legyenek hozzáférhetők a felhasználó számára.⁶¹² Amíg nem áll rendelkezésre az alapértelmezés szerinti adathozzáférés, addig az adatbirtokosoknak kell gondoskodni arról, hogy a felhasználók számára hozzáférhetővé tegyék a könnyen elérhető adatokat, valamint az azok értelmezéséhez és felhasználásához szükséges releváns metaadatokat, éspedig: a) indokolatlan késedelem nélkül, b) az adatbirtokos rendelkezésére

⁶⁰⁹ Data Act (22) preambulumbekkezdés

⁶¹⁰ MIKLÓS Gellért: *Az Európai Unió adatstratégiájához kapcsolódó jogszabályi keretrendszer áttekintése.* Századvég 2022/1. 71.

⁶¹¹ Digitális omnibusz csomag javaslata. Indoklás 5. pont

⁶¹² Data Act 50 cikk és 3. cikk (1) bekezdés

állóval megegyező minőségben, c) könnyen, biztonságosan, díjmentesen, átfogó, strukturált, széles körben használt és géppel olvasható formátumban, és d) folyamatosan és valós időben.⁶¹³ Ugyanezen követelményeknek kell érvényesülni abban az esetben is, ha a felhasználó vagy az ő nevében eljáró fél kérelme alapján harmadik fél részére történik az adatmegosztás.⁶¹⁴

Az ily módon együtt (pl. a gyártó és a felhasználó által) generált adatok tartalmazznak személyes és nem személyes adatokat is, amelyek többnyire elválaszthatatlanok egymástól, ezért a Data Actet együtt kell értelmezni a GDPR-ral, és a következő szabályokat kell figyelembe venni: A Data Act értelmében a felhasználó természetes személyként jogosult hozzáférni az IoT-termék használata által generált valamennyi adathoz; ha a felhasználó egy vállalkozás, akkor adatkezelőnek minősül, ezért ha generált személyes adatokat szeretne kérni, az adatkezeléshez a GDPR szerinti jogalappal kell rendelkeznie. A Data Act önmagában nem képez jogalapot arra, hogy az adatbirtokos személyes adatokat gyűjtsön vagy generáljon.⁶¹⁵

Amennyiben a felhasználók a GDPR szerint érintettnek minősülnek, a Data Act II. fejezetében meghatározott jogok kiegészítik a GDPR 15. cikke szerinti hozzáférési jogokat, valamint a 20. cikke szerinti adathordozhatósághoz való jogokat.⁶¹⁶ Előbbi szerint az érintett jogosult az adatkezelőtől információt kapni személyes adatait illetően, például az adatkezelés céljáról, a tervezett tárolási időről, a címzettekről, akiknek továbbítják az adatokat stb. Utóbbi, tehát az adathordozhatósági jog szerint az érintett jogosult: a) az általa az adatkezelő rendelkezésére bocsátott személyes adatokat széles körben használt, géppel olvasható formátumban megkapni; b) az adatokat egy másik adatkezelőnek továbbítani (ha az említett adatokat automatizált módon kezelik, és érintetti hozzájárulás vagy szerződés alapján kezelik); c) sőt, ha technikailag lehetséges, kérni az adatkezelők közötti közvetlen továbbítást is. A GDPR egyértelműen jelzi, hogy csak az érintett által szolgáltatott adatokról van szó, azt azonban nem határozza meg, hogy ehhez szükség van-e az érintett aktív közreműködésére, és azt sem, hogy alkalmazandó-e olyan helyzetre, amikor passzív módon keletkeznek az adatok, mint például az összekapcsolt termék vagy a kapcsolódó szolgáltatás esetében.⁶¹⁷ Talán ez is hozzájárult ahhoz – amit Tóth András és szerzőtársai állapítottak meg –, hogy az adathordozhatósági jog az egyik legkevésbé sikeres jogintézménye a GDPR-nak.⁶¹⁸

⁶¹³ Data Act 4. cikk (1) bekezdés

⁶¹⁴ Data Act 5. cikk (1) bekezdés

⁶¹⁵ Data Act (7) preambulumbekkezdés

⁶¹⁶ Data Act 1. cikk (5) bekezdés

⁶¹⁷ Data Act (35) preambulumbekkezdés

⁶¹⁸ TÓTH András – SZABÓ Endre Győző – NÉMETH Szabolcs – RUDICS Regina – RIDEG Gergely: *A GDPR és a Digital Markets Act viszonyának tisztázása*. In *Medias Res* 2023/2. 52.

Ugyanakkor éppen a Data Act céljához illeszkedő lehetőséget hordoz magában, és a felhasználóknak is valószínűleg érdemes lesz élni ezzel a jogintézménnyel.

A felsorolt, a GDPR által az érintett számára biztosított adathozzáférési és adathordozhatósági jogokat a Data Act a következőkkel egészíti ki: A Data Act hatálya a személyes és nem személyes adatokra is kiterjed, de nem terjed ki a kikövetkeztetett vagy származtatott adatokra.⁶¹⁹ A felhasználók nemcsak az általuk szolgáltatott személyes adatokhoz férhetnek hozzá, hanem bármely termékadathoz vagy kapcsolódószolgáltatás-adathoz.⁶²⁰ A felhasználók ezeket az adatokat harmadik fél rendelkezésére bocsáthatják, de ezek nem lehetnek a DMA által kapuörnek minősített online platformok.⁶²¹

Mindezen rendelkezések nyomán tehát az IoT-termékek felhasználói hozzáférhetnek, használhatják és megoszthatják azokat az adatokat, amelyeket a termék használatával generálnak, ideértve a személyes és a nem személyes adatokat is. Ezek a jogok azt is mutatják, hogy a jogalkotó a GDPR rendelkezéseit kiegészítette; valamint a releváns fogalmak egy részét is a GDPR-ra utalással határozta meg. A GDPR és a Data Act egységes, koherens rendszert alkot az adatgazdasággal összefüggésben a fogalmak és a szabályozási keretek mentén.

4. Jogeretek az uniós versenyjog és az adatvédelem metszéspontjában

Az ideális helyzet a gazdaság szempontjából az, ha a verseny ösztönzőleg hat rá, a fogyasztók szempontjából pedig az, ha a termékek jobb minőségűek, van választék, és kedvezőek az árak. Ennek biztosítása a versenyjogi szabályok feladata, amelyek nem a versenytársakat, hanem magát a versenyt, a hatékony versenyfolyamatot védik.⁶²² A közösségi versenyjogi szabályok alapjait az EUSZ és az EUMSZ cikkei rögzítik. Előbbi a célokat fogalmazza meg: belső piac létrehozása, gazdasági növekedés, versenyképes piacgazdaság stb.,⁶²³ utóbbi a tilalmakat tartalmazza: verseny megakadályozása, korlátozása vagy torzítása például a vállalkozások közötti megállapodással, az erőfölénnyel való visszaéléssel, tiltott állami támogatással vagy fúziókkal. Mindezek abban az esetben tilosak, ha hatással lehetnek a tagállamok közötti kereskedelemre.⁶²⁴

⁶¹⁹ Data Act (15) preambulumbekkezdés

⁶²⁰ Data Act (35) preambulumbekkezdés

⁶²¹ Data Act (40) preambulumbekkezdés és 5. cikk (3) bekezdés

⁶²² 2009/C 45/02. A Bizottság közleménye – Iránymutatás az EK-Szerződés 82. cikkének az erőfölényben lévő vállalkozások versenykorlátozó visszaélő magatartására történő alkalmazásával kapcsolatos bizottsági jogérvényesítési prioritásokról. 2009. 02. 24. 6. pont

⁶²³ EUSZ 3. cikk (3) bekezdés

⁶²⁴ EUMSZ 101–109. cikk

2023. márciusi adatok szerint a világ legerősebb vállalatai a digitális szektor online platformjai, amelyek általában amerikai vagy ázsiai vállalatok, ebből következően a hasonlóan erős digitális platformmal nem rendelkező EU kedvezőtlenebb pozíciót foglal el a globális adatértékláncban.⁶²⁵ Mindezek háttérében egyrészt az áll, hogy a platformok az EUMSZ 102. cikkét megsértve jellemzően visszaélnék erőfölényükkel;⁶²⁶ másrészt az, hogy 2009 és 2018 között az öt legnagyobb online platform több mint négyszáz felvásárlást hajtott végre világszerte, és egyiket sem tiltották meg.⁶²⁷ Az erőfölénnyel visszaélés trösztellenes vizsgálatokra készítheti a versenyhatóságokat, a tervezett fúzió ellenőrzése – bizonyos feltételek megléte esetén⁶²⁸ – a Bizottság vizsgálatát vonja magával. E vizsgálatok során mind a versenyhatóság, mind a Bizottság gyakran szembesül adatvédelmi kérdésekkel is, ami fölveti a versenyjog és az adatvédelem közötti kapcsolat kérdését.

A továbbiakban egy trösztellenes vizsgálatot és kettő, fúzió engedélyezéséről döntő vizsgálatot tekintek át. Mindhárom ügy elemzése során azt vizsgálom, hogy a piaci versenyben milyen szerepe van a személyesadat-állománynak, valamint hogy az adatvédelmi kérdések mennyiben befolyásolják a versennyel kapcsolatos vizsgálatokat, akár a Bizottság, akár a versenyhatóságok esetében. Ezeket a problémákat sűrítetten és tipikusan hordozzák a bemutatandó ügyek: a Facebook–WhatsApp fúziós ügy, a Facebook (Meta Platforms) kontra Bundeskartellamt trösztellenes ügy és a Google–Fitbit fúziós ügy.

A három ügy bemutatása előtt fontos tisztázni azt, hogy valamely személyesadat-kezelési rendelkezés megsértése önmagában nem versenyjogi probléma, ez az adatvédelmi hatóságok hatáskörébe tartozik. A big data tekintetében azonban annak a tényezőnek is meghatározó súlya van, hogy az érintett vállalkozások nemcsak gyűjtik a személyes adatokat, hanem kezelik, feldolgozzák (következtetések levonása, profil alkotása stb.) és felhasználják saját céljaik érdekében, például az online hirdetési szolgáltatásokban. A big data méretű

⁶²⁵ GORECZKY Péter: *A határokon átnyúló adatáramlás gazdasági szempontjai*. 2024. [A határokon átnyúló adatáramlás gazdasági szempontjai - Világgazdaság \(vg.hu\)](#) (letöltés: 2024. 06. 02.)

⁶²⁶ Gazdasági erejük által versenytársaiktól és fogyasztóiktól nagy mértékben függetlenül tudnak cselekedni, és ezáltal a hatékony versenyt megakadályozni. EBHT 1978. 207. 27/76. sz. United Brands Company és United Brands Continentaal BV kontra Bizottság ügyben hozott ítélet 2. pontja

⁶²⁷ Jason FURMAN et al.: *Unlocking Digital Competition, Report of the Digital Competition Expert Panel*. 2019. 12., 91. https://assets.publishing.service.gov.uk/media/5c88150ee5274a230219c35f/unlocking_digital_competition_furman_review_web.pdf (letöltés: 2024. 01. 02.)

⁶²⁸ A Tanács 139/2004/EK rendelete (2004. január 20.) a vállalkozások közötti összefonódások ellenőrzéséről (a továbbiakban: fúziós rendelet) 1. cikk

adatvagyon és főleg ezek összekapcsolása valamely fúzió során, versenyjogi értelemben piaci értékkel bír.⁶²⁹

4.1. Facebook/WhatsApp ügy⁶³⁰

2014-ben a Bizottság feltétel nélkül engedélyezte, hogy a Facebook felvásárolja a WhatsAppot. A Facebook közösségimédia-szolgáltató és hirdetési szolgáltató, a WhatsApp eredetileg olyan üzenetküldő szolgáltatás, amely hirdetésmentes, és olyan földrajzi területeken is magas a felhasználói fiókkal rendelkezők száma, ahol a Facebook kevésbé népszerű.⁶³¹ A fúzióval fennállt annak lehetősége, hogy a Facebook integrálja a két adatbázist, ezért az összefonódás-ellenőrzés kiterjedt erre a szempontra, de pusztán az online hirdetési piacra és csak az okostelefonokon használható applikációkra vonatkozóan. A Bizottság megállapította egyrészt, hogy ha a WhatsAppon is bevezetnék a célzottreklám-szolgáltatást, az még nem teremtene erőfölényes helyzetet, mert a felhasználók a piacon találhatnak más, hirdetésmentes üzenetküldő szolgáltatást;⁶³² másrészt a felvásárló szerint a Facebook és a WhatsApp felhasználói profiljai egyesítésének jelentős műszaki akadályai vannak, ezáltal a WhatsApp-felhasználók adatait nem tudja felhasználni a Facebookon.⁶³³ A Bizottság egyúttal azt is hangsúlyozta, hogy a személyes adatok védelmével és a magánélettel kapcsolatos aggodalmak nem tartoznak a versenyjogi értékelés szempontjai közé, azok az adatvédelmi szabályok hatálya alá tartoznak.⁶³⁴ Egyetértek a Polyák–Pataki szerzőpáros véleményével, valóban adatvédelmi kérdés az, hogy a Facebook hogyan kezeli a hozzá kerülő személyes adatokat, de az, hogy az összekapcsolt adatbázisokból létrejövő big data léptékű adatvagyon milyen versenyelőnyt jelenthet, mindenképpen körültekintő, alapos versenyjogi vizsgálatot igényelt volna, amit a Bizottság elmulasztott.⁶³⁵ Utóbb a Facebook maga jelezte, hogy összekapcsolta a két adatbázist, és 2017-ben a Bizottság megbírságolta a fúziós rendelet megsértése miatt, tekintetbe véve azt is, hogy félrevezető információt adott az összekapcsolás technikai feltételeiről.⁶³⁶

A fúzió engedélyezése nemcsak versenyelőnyt jelenthet, hanem a versenyelőny következtében a felhasználók kiszolgáltatását is a még nagyobb adatvédelmi és magánéleti

⁶²⁹ POLYÁK Gábor – PATAKI Gábor: *A személyes adatok értéke a Facebook–WhatsApp-összefonódás versenyjogi értékelésében*. Pro Futuro 2018/1. 145.

⁶³⁰ M.7217. sz. ügy – Facebook/WhatsApp

⁶³¹ POLYÁK–PATAKI i. m. 136–137.

⁶³² M.7217. sz. ügy – Facebook/WhatsApp (174) bekezdés

⁶³³ M.7217. sz. ügy – Facebook/WhatsApp (185) bekezdés

⁶³⁴ M.7217. sz. ügy – Facebook/WhatsApp (164) bekezdés

⁶³⁵ POLYÁK–PATAKI i. m. 147.

⁶³⁶ M.8228. sz. ügy – Facebook/WhatsApp. A WhatsApp-felhasználók dönthettek úgy, hogy adataik megosztását nem engedélyezik a Facebook számára.

sérelem lehetőségének. Ha ugyanis a piacon egészséges verseny folyik, akkor a tudatos felhasználóknak van lehetőségük másik közösségi hálózatot vagy másik üzenetküldő szolgáltatást választani, de ha a verseny korlátozott, akkor erre nincs lehetőségük. A big data miatt a Facebook–WhatsApp-fúzió ügyében nem a platform és a felhasználók mint individuumok viszonyán van a hangsúly, hanem a platform és a felhasználói (millió, sőt milliárdos nagyságrendű) közösség viszonya a lényeges. Ilyen értelemben a felhasználókat, a fogyasztókat a versenyjognak is figyelembe kellett volna vennie, hiszen a versenyjog egyik feladata éppen a fogyasztói jólét támogatása. A fogyasztói jólét támogatása, sőt növelése érdekében jelen esetben a Bizottság úgy tudott volna tenni, hogy a fúziók engedélyezésénél figyelembe veszi azt, hogy a döntés mennyiben szolgálja az általános fogyasztói jólétet. A Facebook–WhatsApp-fúziót engedélyező határozat – azzal, hogy a fejlesztés fontos területének nevezi, valamint kiemeli, hogy a felhasználók a fúziós döntés után fokozott adatvédelmet kínáló lehetőségeket kerestek⁶³⁷ – elismeri azt, hogy az adatvédelem és a magánélet védelme a verseny mércéjévé vált. Ez nem azt jelenti, hogy a Bizottság a fúziós döntésekben figyelembe vette ezt a mércét, hiszen határozottan megállapította, hogy a magánélet és a személyesadat-védelem nem tartozik a versenyjogi értékelés szempontjai közé. Itt tátong tehát egy szakadék a verseny mércéje, paramétere és a bizottsági szempontok között.

4.2. Facebook (Meta Platforms) kontra Bundeskartellamt ügy⁶³⁸

A Meta által működtetett Facebook közösségi hálózati szolgáltatást és személyre szabott hirdetési szolgáltatást nyújt. Üzleti modellje szerint előbbi szolgáltatást csak ingyenes regisztrációval lehetett igénybe venni, amely egyúttal a felhasználási feltételek elfogadását is jelentette, vagyis azt, hogy a Facebook nemcsak az adott szolgáltatásból származó adatokat gyűjtötte, hanem más szolgáltatásból, más weboldalakról és alkalmazásokból, cookie-kból stb. származó adatokat is, majd ezeket összekapcsolta a felhasználói fiókkal; s ezt használta fel az egyénre szabott hirdetésekhez. A német versenyhatóság, a Bundeskartellamt 2016-ban eljárást indított a Meta ellen, melynek során az érintett földrajzi és árupiac értékelése által megállapította a Facebook erőfölényes helyzetét, valamint azt, hogy ezzel az adott vállalat a felhasználókra vonatkozó felhasználási feltételei és adatgyűjtési, adatkezelési gyakorlata alapján visszaél, és a németországi közösségi hálózatok piacán fennálló erőfölénye visszaélésszerű kihasználása miatt – a versenykorlátozás tilalmáról szóló német törvény 19. §

⁶³⁷ M.7217. sz. ügy – Facebook/WhatsApp (87) bekezdés és 79. lj.

⁶³⁸ C-252/21. sz. ügy – Meta Platforms/Bundeskartellamt

(1) bekezdése alapján, amely tiltja a vállalatok erőfölénnyel visszaélését – határozatban tiltotta meg a Facebooknak a felhasználási feltételek szerinti adatkezelést, valamint arra kötelezte, hogy az alapszolgáltatáson kívül gyűjtött adatok kezeléséhez külön-külön szerezze be az érintettek hozzájárulását.⁶³⁹ A Meta fellebbezést nyújtott be a düsseldorfi felsőbírósághoz, és azt a hatóságok hatáskör-keveredésére alapozta, vagyis arra, hogy a nemzeti versenyhatóságok kompetenciájába nem tartozik bele annak ellenőrzése, hogy az adatkezelés megfelel-e a GDPR-nak. A felsőbíróság helyt adott a fellebbezésnek – mert a felhasználók megismerhetik és dönthetnek a felhasználási feltételek el- vagy el nem fogadásáról –, és felfüggesztette a német versenyhatóság határozatának végrehajtását. A felfüggesztés elleni fellebbezést követően a német szövetségi felsőbíróság eltekintett az adatvédelmi szál elemzésétől, és versenyjogi szempontok alapján döntött: mivel nincs a Facebooknak versenytársa, a felhasználók kénytelenek a felhasználási feltételeket elfogadni, ha a közösségi hálózatot használni akarják. Az ügy következő fontos állomása az, hogy a düsseldorfi regionális felsőbíróság előzetes döntéshozatal iránti kérelmet nyújtott be az EUB-hez, melyre 2022-ben indítvány, majd a következő évben bírósági ítélet⁶⁴⁰ született.

A Facebook kontra Bundeskartellamt ügyből – a versenyjog és adatvédelem összefonódása szempontjából – két fő kérdéskör megvilágítása szükséges: egyrészt a versenyhatóság kompetens-e az általa vizsgált magatartásoknak a GDPR szabályaival való összeegyeztethetőségét illetően; másrészt a személyes adatok kezelésének jogszerűsége és annak összefüggése a versenyjoggal.

Az első kérdéskörre vonatkozóan – amely rendszerszintű problémát takar – az EUB-ítélet szerint, hogyha szükséges az erőfölényes gazdasági szereplő visszaélésszerű magatartásának megállapításához az adatvédelmi szempontok vizsgálata, akkor ezt – a lojális együttműködésre vonatkozó kötelezettségek betartása mellett – a tagállami versenyhatóság megteheti, és megállapíthatja a jogsértést a GDPR vonatkozásában.⁶⁴¹ A szükségesség kérdésének eldöntését a versenyhatóságokra bízta. A lojális együttműködés elvét az EUSZ írja elő, ennek értelmében az EU és a tagállamok, azok hatóságai tiszteletben tartják és segítik egymást a feladatok végrehajtásában,⁶⁴² ennek kereteit, konkrét szabályait – a nemzeti versenyhatóságok és a GDPR szerint illetékes nemzeti felügyeleti vagy a fő felügyeleti hatóságok vonatkozásában – azonban egyetlen uniós jogi aktus sem határozza meg. A konkrét

⁶³⁹ Bundeskartellamt B6-22/16. sz. határozata, 2019. február 06.

⁶⁴⁰ EUB-ítélet C-252/21. sz. ügy

⁶⁴¹ EUB-ítélet C-252/21. sz. ügy 62. pont

⁶⁴² EUSZ 4. cikk (3) bekezdés

teendőket az EUB-ítélet a következők szerint állapítja meg: A nemzeti versenyhatóságnak ellenőriznie kell, hogy a vizsgálandó magatartás vagy hasonló magatartás képezte-e már tárgyát az illetékes nemzeti felügyeleti hatóság, a fő felügyeleti hatóság vagy az EUB határozatának; s ha igen, akkor attól nem térhet el.⁶⁴³ E kötelezettségnek az a célja, hogy a korábbi esetek által az egységes megközelítést tegye lehetővé, elkerülve annak kockázatát, hogy a versenyhatóság és az adatvédelmi felügyeleti hatóság eltérően értelmezze a GDPR-t. Ha ezen ellenőrzés során a versenyhatóságnak kétségei támadnak az illetékes felügyeleti hatóság vagy a fő felügyeleti hatóság által végzett értékelés terjedelmével, vagy ha adott magatartást e hatóságok egyidejűleg vizsgálják, vagy még nem végeztek adott magatartásra vonatkozó vizsgálatot, akkor a nemzeti versenyhatóságnak konzultálnia kell e hatóságokkal, és együttműködésüket kell kérnie annak érdekében, hogy eloszlassa kétségeit, vagy eldöntse, hogy meg kell-e várnia az érintett felügyeleti hatóság határozatának meghozatalát, mielőtt megkezdene saját értékelésének elvégzését.⁶⁴⁴ A konzultálás és az együttműködés kérése azért fontos, mert az adatvédelemnek nincs központi uniós hatósága, így a nemzeti felügyeleti hatóság a felelős a GDPR alkalmazásának ellenőrzéséért, valamint a versenyhatóság ezáltal felelhet meg maximálisan az adott ügy értelmezésével kapcsolatban a gondos ügyintézés elvének. Amennyiben a megkeresett hatóság nem emel kifogást, vagy észszerű határidőn belül⁶⁴⁵ nem válaszol, a nemzeti hatóság folytathatja saját vizsgálatát.⁶⁴⁶ A Facebook kontra Bundeskartellamt ügyben a német versenyhatóság eleget tett a lojális együttműködés kötelezettségének az ügyben illetékes valamennyi adatvédelmi felügyeleti hatóság vonatkozásában.⁶⁴⁷

A Facebook kontra Bundeskartellamt ügy kapcsán – azon túl, hogy adatvédelmi kérdésekben van-e hatásköre a versenyhatóságnak – abban a tekintetben (második kérdéskör) is fölmerült az adatvédelem és a versenyjog összefonódása, hogy a személyes adatok kezeléséhez milyen jogalapra hivatkozhat a Facebook. Szerződés teljesítéséhez szükséges, a jogos érdek és az érintett hozzájárulása jöhet szóba.⁶⁴⁸ Szerződés teljesítéséhez akkor szükséges az adatkezelés, ha az érintett az egyik szerződő fél, és az adatkezelés objektíve elengedhetetlen, vagyis a szerződés fő célja ezen adatkezelés hiányában elérhetetlen.⁶⁴⁹ Lényegében hasonló magyarázatot tartalmaz az EDPB vonatkozó iránymutatása, és kiemeli, hogy az adatkezelés

⁶⁴³ EUB-ítélet C-252/21. sz. ügy 56. pont

⁶⁴⁴ EUB-ítélet C-252/21. sz. ügy 57. pont

⁶⁴⁵ Az EJEB ítélkezési gyakorlata alapján az eset egyedi körülményei határozzák meg, melynek kritériumai: az eset bonyolultsága, a kérelmező és a releváns hatóságok magatartása és a tétje a kérelmező számára.

⁶⁴⁶ EUB-ítélet C-252/21. sz. ügy 63. pont

⁶⁴⁷ EUB-ítélet C-252/21. sz. ügy 60. pont

⁶⁴⁸ GDPR 6. cikk (1) bekezdés a), b) és f) pontok

⁶⁴⁹ EUB-ítélet C-252/21. sz. ügy 98. pont

szükségessége és hasznossága nem ugyanazt jelenti, még akkor sem, ha az az adatkezelő egyéb üzleti céljaihoz szükséges,⁶⁵⁰ sőt, kimondja, hogy az online profilalkotáshoz és hirdetésekhez nem megfelelő ez a jogalap.⁶⁵¹ Az EUB-ítélet maga is azt sugallja, hogy az EUB a tartalmak személyre szabását vagy a Meta-csoport szolgáltatásainak zökkenőmentes használatát semmiképpen nem sorolja a szükséges kategóriába,⁶⁵² ez inkább a platform egyoldalú nézőpontja.

A hirdetések személyre szabása – mint a jogos érdek célja – ugyan elvileg indokolhatná az adatkezelést, de az adatkezelés tekintetében jogos érdekre csak akkor hivatkozhatna a Facebook, ha: a) az adatvédelemmel érintett személy alapvető jogai és szabadságai nem magasabb rendűek az adatkezelő jogos érdekénél; b) ha az érvényesíteni kívánt jogos érdek észszerűen nem érhető el a magánélet tiszteletben tartásához és a személyes adatok védelméhez való jogukat kevésbé veszélyeztető eszközök révén; s ezeken túlmenően az adattakarékosság elvére is figyelemmel kell lenni.⁶⁵³ A fentiek alapján az EUB-ítélet a jogos érdeket sem tartja a Facebook esetében jogszerű jogalapnak.

A személyes adatok kezelésének a Facebook esetében tehát egyetlen jogszerű jogalapja maradt: az érintett hozzájárulása, amelyet a Facebook úgy szerzett meg, hogy a közösségi hálózati szolgáltatás – amelyet ingyenes regisztrációhoz kötött – felhasználói feltételeinek elfogadásához kötötte, vagyis a felhasználók egyúttal ahhoz is hozzájárultak, hogy a Facebook ne csak a közösségi hálózati szolgáltatásból származó személyes adatokat gyűjtse, hanem más szolgáltatásokból, harmadik felek weboldalairól és alkalmazásaiból, cookie-kból stb. származó adatokat is, és ezeket, összekapcsolva a felhasználói fiókkal, felhasználja a személyre szabott hirdetésekhez. Az érintett hozzájárulása azonban csak abban az esetben érvényes, ha azt önkéntesen adta, félreérthetetlenül jelezve, hogy beleegyezik az őt érintő személyes adatok kezelésébe.⁶⁵⁴ Az EUB-ítélet szerint az önkéntességet, ezáltal az érvényességet önmagában nem zárja ki a Facebook erőfölényes helyzete, de mivel az erőfölényes helyzet egyértelműen egyenlőtlen viszonyt, egyensúlyhiányt teremt a Facebook és a felhasználók között – tekintve, hogy nincs más közösségi hálózati szolgáltatás –, ez érintheti a felhasználók választási szabadságát, ami befolyással lehet a hozzájárulás önkéntességére és érvényességére.⁶⁵⁵ Emellett

⁶⁵⁰ EDPB: 2/2019. iránymutatás a személyes adatoknak az általános adatvédelmi rendelet 6. cikke (1) bekezdésének b) pontja szerinti kezeléséről az érintettek részére nyújtott online szolgáltatások összefüggésében. 2.0 változat. 2019. október 8. 25. pont

⁶⁵¹ EDPB: 2/2019. 51. pont

⁶⁵² EUB-ítélet C-252/21. sz. ügy 103. pont

⁶⁵³ EUB-ítélet C-252/21. sz. ügy 105–109. pont

⁶⁵⁴ GDPR 4. cikk 11. pont

⁶⁵⁵ EUB-ítélet C-252/21. sz. ügy 142–154. pont

az önkéntesség megállapítása során fontos annak figyelembevétele, hogy szolgáltatások nyújtására vonatkozó szerződés teljesítésének feltételül szabták-e az olyan, személyes adatok kezeléséhez való hozzájárulást, amelyek nem szükségesek a szerződés teljesítéséhez.⁶⁵⁶ Az adatvédelmi és a versenyjogi jogsértés összefonódása nem zárja ki azt a lehetőséget, hogy akár mindkét hatóság eljárjon adott ügyben. Ezt még a ne bis in idem, azaz a kétszeres értékelést tiltó elv sérelme sem korlátozza, ha – a Charta 52. cikke alapján – a bírságkiszabást minimum törvényszintű jogszabály írja elő, más jogalapon indult a két eljárás, arányos és elengedhetetlen; vagyis ha a hatóságok figyelembe veszik a másik által kiszabott bírságot.⁶⁵⁷

Az előzetes döntéshozatal iránti kérelemre született EUB-ítélettel még nem zárult le a Facebook kontra Bundeskartellamt ügy, hiszen az EUB nem dönti el a tagállami bíróság előtti jogvitát. A továbbiakban a kérelmet benyújtó bíróságnak kell a döntést meghoznia, amelynek során az EUB iránymutatásait figyelembe kell vennie. Ebben az esetben a Meta visszavonta a versenyhatóság határozata elleni fellebbezését, a megelőző tárgyalások során olyan vállalásokat tett, amelyek a felhasználók számára erőteljesebb ellenőrzést biztosítanak adataikkal kapcsolatban.⁶⁵⁸ Az EUB-ítélet nemcsak az adott Facebook-ügyre vonatkozóan tartalmaz iránymutatást, hanem hatással lesz a hasonló kérdésekben eljáró hatóságokra és bíróságokra. A piaci erőfölénnyel való visszaélés vizsgálata igazolhatja a versenyjog hatálya alá nem tartozó olyan normáknak a versenyhatóság általi értelmezését, mint a GDPR. Ez a kérdéskör a DMA hatályba lépése miatt annyiban jelentőségét veszítette, hogy az alapvetően tiltja⁶⁵⁹ a kapuőröknek az alapszolgáltatásukból származó személyes adatok összekapcsolását, kombinálását, keresztfelhasználását a más forrásból származó adatokkal, valamint a személyes adatok összekapcsolása céljából nem léptethetik be a végfelhasználókat más szolgáltatásaikba. E tilalom alól egyetlen kivételt állapít meg: a felhasználó hozzájárulását.

A DMA adatvédelmet erősítő rendelkezéseivel részleges választ ad a versenyhatóság adatvédelmet érintő hatásköri problémáira, ugyanakkor teljes egészében nem oldja azt meg, hiszen a DMA csak a kapuőrökre vonatkozóan állapít meg kötelezettséget és tiltásokat, de erőfölényes vállalat rajtuk kívül is létezik, így valószínű, hogy a versenyhatóságok számára értékes információkat jelent az előzetes döntéshozatal iránti kérelemre született EUB-ítélet. Az

⁶⁵⁶ GDPR 7. cikk (4) bekezdés

⁶⁵⁷ GÖNCZÖL Tünde – TELEKI Lóránt: *A digitális kapuőrök az ex ante szabályozás, a versenyjog és az adatvédelem keresztműzében*. In: VALENTINY Pál et al. (szerk.): *Verseny és szabályozás, 2022*. Bp., MTA Közgazdaság- és Regionális Tudományi Kutatóközpont Közgazdaság-tudományi Intézet, 2023. 261.

⁶⁵⁸ Bundeskartellamt: Facebook proceeding concluded. Sajtóközlemény, 2024. 10. 10. https://www.bundeskartellamt.de/SharedDocs/Meldung/EN/Pressemitteilungen/2024/10_10_2024_Facebook.html (letöltés: 2025. 01. 10.)

⁶⁵⁹ DMA 5. cikk (2) bekezdés

ebben felsorolt kötelezettségek tulajdonképpen az EUSZ által előírt együttműködés kötelező lehetőségeit tárják fel – ezt az EDPB is megerősítette⁶⁶⁰ –, ily módon pótolják a különböző közigazgatási hatóságok és a GDPR szerinti felügyeleti hatóságok együttműködésére vonatkozó pontos szabályok hiányát a GDPR-ban; ill. tágabb összefüggésben kijelölik az utat a versenyhatóságok és az adatvédelmi hatóságok hatáskörének metszéspontját érintő kérdésekben. Egyelőre nincs intézményesített megoldás a két terület együttműködésére, még ha eseti párbeszéd és tagállami soft law eszközök léteznek is. Az említett ítélet kiindulóalapként szolgálhat az együttműködés valamely formájának megvalósításához, például az adatvédelmi hatóság bevonása a versenyhatósági vizsgálatba; konzultációs szervezet létrehozása a két hatóság együttműködésére vonatkozóan, amely a folyamatban lévő ügyekhez tanácsadói jogkörrel lenne felruházva; sőt, akár speciális bíróság felállítása is szóba jöhetne abban az esetben, ha a DMA nem kezelné hatékonyan a problémákat, ill. ha a DMA hatályán kívül eső ügyek nagy számban fordulnak elő.

Az adatkezelés jogszerűsége alapvetően adatvédelmi kérdés, az EUB is a GDPR alapján válaszolja meg a konkrét kérdéseket. Versenyjogi relevanciával annyiban bír, hogy a konkrét ügyben erőfölényes vállalatról van szó, amely a platformok sajátos, tipikus logikája mentén működik. Ezek a tények késztették arra az EU-t, hogy a digitális piacokon kapuőröket jelöljön ki, amelyek számára csak a felhasználó hozzájárulása szolgálhat jogalapként, és tiltja a más jogalapra hivatkozást.⁶⁶¹ A jogalapok, ezen belül a hozzájárulás önkéntességének vizsgálata azonban azt is prezentálja, hogy az alapvetően személyesadat-kezelési kérdések megvilágítása is kívánhat versenyjogi szempontú elemzést. A Facebook (Meta) kontra Bundeskartellamt ügy rámutat arra, hogy a felhasználók önkéntes hozzájárulásának vizsgálatához az egyenlőtlen viszony fennállásának elemzése is hozzátartozik; ez pedig azt jelenti, hogy az adatvédelmi hatóságok „kirándulást tehetnek” a versenyjog területére.⁶⁶²

A versenyhatóságok adatvédelmi vizsgálatainak szükségessége, és fordítva, az adatvédelmi hatóságok versenyjogi kitekintésének szükségessége magyarázható azzal, hogy a személyes adatok üzleti célú gyűjtése, adatvagyonként kezelése nem csupán személyesadatvédelmi kérdés, hanem központi szerepet kap az adatgazdaságban, a piaci versenyben, az innovációban, a teljes ökoszisztémában, amely a vonatkozó jogszabályok által felveti a hatóságok közötti munkamegosztás hagyományos kereteinek szétfeszítését is. Az adatvédelmi

⁶⁶⁰ EDPB: Állásfoglalás az adatvédelem és a versenyjog közötti kölcsönhatásról. 7–8.

⁶⁶¹ DMA 5. cikk (2) bekezdés d) pont

⁶⁶² PÓK László: *Az Európai Bíróság újabb Meta-ügyben hozott döntése: bajban az online hirdetési szektor?* Blogbejegyzés, 2023. július 7. https://gdpr.blog.hu/2023/07/07/az_europai_birosag_ujabb_meta-ugyben_hozott_dontese_bajban_az_online_hirdetesi_szektor (letöltés: 2024. 02. 02.)

gyökerek miatt több területen érintett online platformok tekintetében a hatóságoknak jogosultsággal kell rendelkezniük ezek vizsgálatára is.

4.3. Google/Fitbit ügy⁶⁶³

2020-ban a Bizottság engedélyezte a Fitbit, testen viselhető eszközöket gyártó vállalat felvásárlását a Google számára. Előtte vizsgálta és értékelte⁶⁶⁴ a fúziót, amelynek során figyelembe vette, hogy a Fitbit profiljából adódóan a tranzakció nagy mennyiségű érzékeny személyes adatot, egészségügyi adatot érint. A Bizottság a vizsgálat után a következő, piaci versenyre vonatkozó aggályokat fogalmazta meg:⁶⁶⁵ 1.) A Google a Fitbit-felhasználók egészségi állapotának, fittségének adatbázisát egyesítve a sajátjával, lehetetlenné teheti a versenytársak piacra jutását és terjeszkedését az online hirdetési szolgáltatások területén, amely magasabb árakat jelenthet a hirdetők számára a kvázi horizontális kárelméleti⁶⁶⁶ megközelítés alapján. 2.) A piac számos szereplője az API-n (alkalmazásprogramozási felületen)⁶⁶⁷ keresztül fér hozzá a Fitbit által biztosított egészségügyi és fitneszadatokhoz, a felvásárlást követően azonban a Google korlátozhatja a versenytársak hozzáférését az API-hoz, ez pedig sértené a versenyt a digitális egészségügyi piacokon. 3.) A Google hátrányos helyzetbe hozhatja a csuklón hordható eszközök konkurens gyártóit azáltal, hogy korlátozza az Android okostelefonokkal való kompatibilitásukat.

Mivel azonban a digitális egészségügyi szektor még mindig kialakulóban van, és számos aktív versenytárs van ezen a területen, a Bizottság elfogadta az aggályok orvoslása érdekében a Google által felajánlott kötelezettségvállalásokat: 1.) Külön adatsilóban tárolja az EGT-ben élő felhasználók Fitbit-eszközeiről gyűjtött adatokat, ezáltal elkülöníti a többi Google-adattól, és ezeket nem használja fel hirdetési céllal, csak kifejezett felhasználói hozzájárulás alapján. 2.) A felhasználók továbbra is hozzáférhetnek az API-n adataikhoz és a

⁶⁶³ M.9660. sz. ügy – Google/Fitbit

⁶⁶⁴ Fúziós rendelet 1–2. cikk alapján

⁶⁶⁵ EC.EUROPA.EU: *Commission clears acquisition of Fitbit by Google, subject to conditions*. Sajtóközlemény, 2020. december 17. [Mergers: Commission clears acquisition of Fitbit by Google \(europa.eu\)](https://ec.europa.eu/competition/mergers/decisions/mrg_2020_17_en) (letöltés: 2022. 11. 10.)

⁶⁶⁶ GCR (Global Competition Review): *Crucial Developments to European Data and Privacy in Merger Control*, 2023. december 08. <https://globalcompetitionreview.com/guide/digital-markets-guide/third-edition/article/crucial-developments-european-data-and-privacy-in-merger-control#footnote-009> (letöltés: 2024. 01. 12.)

⁶⁶⁷ Az API használatával a Fitbit-felhasználó megoszthatja adatait más alkalmazásokkal, amelyek – a felhasználó engedélyezése után – hozzáférhetnek az adatokhoz. Így a futásról, kerékpározásról stb. megosztott adatai alapján a fizikai aktivitására, egészségére vonatkozó információhoz juthat.

szoftveralkalmazásokhoz. 3.) A csuklón hordható eszközök⁶⁶⁸ és az okostelefonok Android operációs rendszerének interoperabilitását megőrzi, beleértve a frissítéseket is. Ezen vállalatok adatgyűjtési és adatkezelési elvei azóta bekerültek a DMA⁶⁶⁹ rendelkezései és tiltásai közé, ez további kényszerítőerővel bír a Google számára kötelezettségvállalásainak betartására.

A döntés során a viták nagy része arra irányult, hogy a tervezett fúzió mennyiben érinti a személyes adatok és a magánélet védelmét. Az EDPB nyilatkozatban fogalmazta meg véleményét, és jelezte, hogy készen áll arra, hogy az egyesüléssel kapcsolatos tanácsaival a Bizottság rendelkezésére álljon, ha erre kéri.⁶⁷⁰ A felvásárlással a Fitbit-felhasználók kevésbé tudják nyomon követni egészségügyi adataik további felhasználását, ami a magánélet sérüléséhez vezethet. Ez újra fölveti azt a kérdést, hogy a magánélet sérülése ellen a versenyjognak védenie kell-e, s ha igen, milyen mértéken. A Bizottság azt az álláspontot képviselte, hogy ebben az esetben nem, mert ez a GDPR feladata, másrészt a magánélet esetleges sérelme nem a verseny következménye. A döntést követő sajtóközlemény szavaival élve: „Az ilyen aggályok nem tartoznak a fúzióellenőrzés hatáskörébe, és vannak olyan szabályozási eszközök, amelyek alkalmasabbak ezek kezelésére.”⁶⁷¹ Más szóval, a Bizottság a magánélet, a magánszféra védelmét továbbra is csak a verseny egyik lehetséges paraméterének tekinti, de nem az uniós összefonódás-ellenőrzés által önmagában védendő dolognak tartja.⁶⁷²

4.4. A versenyjogi ügyek idővonala

A 6. táblázat a fontosabb versenyjogi ügyek idővonalát szemlélteti (mutatva az előzőekben elemzett ügyeket is), valamint az általuk felvetett adatvédelmi problémát, és ezzel kapcsolatban a Bizottság vagy a versenyhatóság álláspontját foglalja össze.

6. táblázat: Fontosabb versenyjogi ügyek, amelyekben a személyes adatok érintettek

Ügy	Ügytípus	Év	Adatvédelmi probléma mint a vizsgálat tárgya	Bizottság/versenyhatóság állásfoglalása
-----	----------	----	--	---

⁶⁶⁸ A felajánlott kötelezettségvállalások közé csak a csuklón hordható fitneszeszközök tartoznak, de az érintett termékpiacon léteznek más testrészen hordható eszközök (gyűrűk, ruhák) is. A jogorvoslatok nem terjednek ki ennek a módosítására.

⁶⁶⁹ DMA 5–6. cikk

⁶⁷⁰ EDPB: Statement on privacy implications of mergers Adopted on 19 February 2020. https://www.edpb.europa.eu/sites/default/files/files/file1/edpb_statement_2020_privacyimplicationsofmergers_en.pdf (letöltés: 2022. 02. 12.)

⁶⁷¹ Ec.europa.eu: Commission clears acquisition of Fitbit by Google... i. m.

⁶⁷² Simon VANDE WALLE: *The European Commission Clears the Acquisition of a Maker of Fitness Trackers and Smartwatches by a Major Online Platform, Subject to Long-Lasting Behavioural Remedies* (Google/Fitbit, M.9660) (September 2, 2021). *Concurrences Competition Law Review* 2021/3. 126. <https://ssrn.com/abstract=3915946> (letöltés: 2024. 02. 02.)

M.4731. – Google–DoubleClick	fúzió engedélyezve	2008	- online hirdetési szolgáltatások ötvözése hirdetiskiszolgáló rendszerrel (grafikus megjelenítés) - ügyfelek adataihoz hozzáférés	az engedélyezés nem érinti a a felekre rótt kötelezettségeket az egyének védelme és a magánélet védelme tekintetében
AT.39740. – Google Search (Shopping) T-612/17. Törvényszék C-48/22. P. főtanácsnok indítványa	antitrösztvizsgálat: erőfölénnyel visszaélés bizottsági határozat: erőfölénnyel visszaélés megállapítása Google-kereset elutasítása fellebbezés elutasítását, a bizottsági határozat, pénzbírság helybenhagyását javasolja	2010 2017 2021 2024	- piacerő-átvitel, önpreferálás - ingyenes szolgáltatás → a felhasználók adataikkal fizetnek → hozzájárulnak a bevételhez	- verseny megakadályozása → valódi választás lehetőségét elvette a fogyasztóktól
M.7217. Facebook–WhatsApp M.8228. Facebook–WhatsApp	fúzió (feltétel nélkül) engedélyezve de: félrevezető információ ↓ fúziós rendelet megsértése → bírság	2014 2017	- WhatsApp felhasználók személyes adatainak összekapcsolása a Facebookkal → online hirdetési szolgáltatás céllal	- az aggályok nem a versenyjogi, hanem az adatvédelmi szabályok hatálya alá tartoznak
Facebook (Meta)/ Bundeskartellamt B6-22/16. C-252/21.	antitrösztvizsgálat: erőfölénnyel visszaélés ↓ Bundeskartellamt stb. ↓ előzetes döntéshozatal iránti kérelem ↓ EUB-ítélet Bundeskartellamt–Meta tárgyalások ↓ a Meta visszavonta fellebbezését	2016 2019– 2021 2023 2024	- felhasználási feltételek - személyes adatok jogalap nélküli gyűjtése → összekapcsolásuk → online hirdetési szolgáltatás céllal	az adatvédelmi hatósággal együttműködve végezhet vizsgálatot, és megállapíthatja a jogsértést a GDPR vonatkozásában (de: lojális együttműködés)
M.9660. Google–Fitbit	fúzió (felajánlott kötelezettségvállalással) engedélyezve	2020	- adatok kombinálása → online hirdetési szolgáltatás céllal → a felhasználók kevésbé tudják adataikat követni	- az adatvédelem a verseny egyik paramétere - az aggályok nem tartoznak a fúzióellenőrzés hatáskörébe

			- API-használat korlátozása - korlátozhatja más gyártók eszközeinek az Android telefonokkal való kompatibilitását	- vannak alkalmasabb eszközök
AT.40684. Facebook– Marketplace	antitrösztvizsgálat: erőfölénnyel visszaélés (Bizottság kifogásközlése) ↓ bizottsági határozat: erőfölénnyel visszaélés megállapítása (árkapcsolás)	2021 2022 2024	- a Marketplace és a Facebook adatainak összekapcsolása → online hirdetési szolgáltatás céllal - versenytársak adatainak használata a saját hirdetésekben	döntésében figyelembe veszi a hirdetésekhez kapcsolódó, harmadik felek által generált adatok szerepét
AT.40670. – Google	antitrösztvizsgálat: erőfölénnyel visszaélés (Bizottság kifogásközlése) ↓ bizottsági határozat: erőfölénnyel visszaélés megállapítása (versenytársak kizárása)	2021 2023 2025	- saját hirdetések előnyben részesítése - hirdetés céljából harmadik felek felhasználói adatokhoz való hozzáféréseinek korlátozása	az adatokhoz való egyoldalú hozzáférés és azok elzárása a versenytársaktól a piaci erőfölénnyel való visszaélés egyik formája

Forrásai: Unió versenyügyek keresőfelülete: <https://competition-cases.ec.europa.eu/search?search=m.9660&sortField=relevance&sortOrder=DESC> (letöltés: 2024. 12. 20.); továbbá: T-612/17. – Törvényszék: 62017TJ0612; C-48/22. P. Főtanácsnok indítványa: Document 62022C C0048.; Meta Platforms/Bundeskartellamt: B6-22/16, Document 62021CJ0252., EUB-ítélet C-252/21. sz. ügy, Bundeskartellamt: Facebook proceeding concluded; Facebook–Marketplace: <https://competition-cases.ec.europa.eu/cases/AT.40684> (letöltés: 2025. 01. 10.), European Commission: Commission fines Meta €797.72 million over abusive practices benefitting Facebook Marketplace. Sajtóközlemény, Brüsszel, 2024. 11. 14. https://ec.europa.eu/commission/presscorner/api/files/document/print/en/ip_24_5801/IP_24_5801_EN.pdf (letöltés: 2025. 01. 10.); European Commission: Commission sends Statement of Objections to Google over abusive practices in online advertising technology. Sajtóközlemény, 2023. június 14. https://ec.europa.eu/commission/presscorner/detail/en/ip_23_3207 (letöltés: 2024. 12. 02.); European Commission: Commission fines Google €2.95 billion over abusive practices in online advertising technology. Sajtóközlemény, 2025. szeptember 5. https://ec.europa.eu/commission/presscorner/detail/en/ip_25_1992 (letöltés: 2025. 12. 31.)

4.5. A versenyjogi ügyek tapasztalatai

A fúziók legproblémásabb eleme az adatbázisok egyesítése volt, hiszen később az adatok feldolgozása, a platform céljainak megfelelően, például algoritmusokkal, és felhasználása az online hirdetési szolgáltatásokban, hozzájárult ahhoz, hogy adott platform képes legyen visszaélni erőfölényével. A fúziók előzetes vizsgálatában az adatvagyon vizsgálata kell álljon középpontban, de nem mint adatvédelmi összetevő, hanem mint versenyelőny, mint a versenykorlátozó magatartás kiváltó oka. A fúziós ügyek a Bizottság merev szemléletét mutatják, amely ugyan elismeri, hogy a személyes adatok és a magánélet védelme a verseny egyik lehetséges összetevője, de a velük kapcsolatos aggodalmakat a konkrét

ügyekben az adatvédelmi hatóságok kompetenciájába tartozónak ítéli, és döntéseiben nem veszi figyelembe.

A trösztellenes ügyek azt mutatják, hogy a személyes adatok kezelésének gyakorlata olyan adatvagyonhoz és ezáltal erőfölényhez juttatta a platformokat, amellyel képesek visszaélni. A Facebook (Meta) kontra Bundeskartellamt ügyben a német versenyhatóság, a Bundeskartellamt döntését emelem ki, amely kimondta, hogy a Facebook visszaél piaci erőfölényével, és ezt a felhasználási feltételei által teheti meg.⁶⁷³ Lényegében hasonló következtetéseket fogalmaz meg az előzetes döntéshozatali kérelem kapcsán született EUB-ítélet is. Leszögezi egyrészt, hogy a versenyhatóságok – a lojális együttműködés kötelezettsége mellett – megállapíthatnak jogsértést a GDPR vonatkozásában, ha ez szükséges az erőfölénnyel visszaélés fennállásának bizonyításához;⁶⁷⁴ másrészt az adatkezelés jogszerűsége tekintetében a GDPR alapján válaszolja meg a felmerült kérdéseket. Az antitrösztvizsgálatok tapasztalatai kikristályosították azokat a versenyjogi problémákat, amelyek elvezettek a platformok célzott szabályozásáig, így a DMA-rendelkezések végeredményben visszamenőlegesen igazolják is a Facebook (Meta) kontra Bundeskartellamt ügyből levonható következtetéseket.

Az összefonódás-ellenőrzési és versenyhatósági ügyek idővonala, ill. az ügyek adatvédelmi kitettsége alapján 2016-2017 körül látható a fordulópont – amikor nyilvánvalóvá vált a Facebook valódi szándéka a WhatsApp felvásárlásával, és az elégtelen bizottsági vizsgálat következménye is –, amely időtől a döntéshozók óvatosabban járnak el a hasonló ügyekben. Ettől kezdve rajzolódik ki az a folyamat is, ami, tanulva a nagy ügyek tapasztalataiból, elvezetett az ex ante szabályozás melletti döntéshez,⁶⁷⁵ és végül 2022-ben a DMA végleges normaszövegéhez. A DMA a kapuőrök kijelölésével reagál a korábban felvetődött, adatokkal kapcsolatos versenyjogi kihívásokra, amivel elméletileg képes támadhatóvá tenni e piacokat, és képes az erőfölénnyel visszaélés megfékezésére.

A DMA nemcsak a trösztellenes vizsgálatokat spórolja meg a kapuőrök vonatkozásában, hanem a fúziókra vonatkozóan is rendelkezik. A továbbiakban a kapuőrnek előzetesen be kell jelentenie az Európai Bizottságnak minden olyan tervezett fúziót, amelyben a részt vevő felek lehetővé teszik az adatgyűjtést, alapvető platformszolgáltatást vagy a digitális ágazatba tartozó bármely egyéb szolgáltatást nyújtanak.⁶⁷⁶

⁶⁷³ Bundeskartellamt B6-22/16.

⁶⁷⁴ EUB-ítélet C-252/21. sz. ügy 62. pont

⁶⁷⁵ A digitális platformok megfékezésére többféle lehetőség áll rendelkezésre, a legagresszívabb feldarabolástól kezdve, a fúziók felülvizsgálatán át a hagyományos versenyjogi szabályozás különböző mértékű reformjáig. TÓTH András: *A technológiai óriások piaci megregulálásának versenyjogi mozgatói és aspektusai, különös tekintettel a Digital Markets Act javaslatra*. Versenytükör 2021/1. 54.

⁶⁷⁶ DMA 14. cikk

5. Összegzés és következtetés

Az online platformok – megkerülve a GDPR rendelkezéseit vagy kihasználva a közös európai adatvédelmi együttgondolkodás hiányát – a személyes adatok kezelése, kumulációja által piaci erőfölényre tesznek szert, amivel egyre erőteljesebben visszaélnek. Az EUMSZ 102. cikke alapján a trösztellenes ügyekben eljáró versenyhatóságok, a fúziók engedélyezésében a Bizottság vizsgálatai fölvetették a személyes adatok és a magánélet védelmével kapcsolatos aggodalmakat, de a 2017-ig pusztán adatvédelmi problémának tekintve elvetették ezeknek a versenyre és a piaci erőfölényre gyakorolt hatását, s majd csak a Facebook–WhatsApp-fúzió engedélyezése után kezdtek megfontoltabban és körültekintőbben gondolkodni. Nem sokkal később a németországi Facebook-ügyben eljáró Bundeskartellamt döntése erősítette meg az adatvédelmi és a versenyjogi szál összefonódását, úgy, mint ok-okozati összefüggést, és úgy is, mint a két hatóság együttműködésének elkerülhetetlenségét, amit a kapcsolódó előzetes döntéshozatali kérelemre született EUB-ítélet is megerősített. Ez az első állásfoglalás, amely a lojális együttműködésen alapuló feltételek teljesülése esetén a versenyhatóságok számára is lehetővé teszi személyesadat-védelmi kérdésekben a vizsgálódást és megállapítások tételét. Az ügyek tapasztalatai hozzájárultak a DMA jogalkotási aktusához,⁶⁷⁷ amely rendeleti formában, ex ante eszközökkel reagál a digitális gazdaságban a kapuőrök adatkezeléssel összefüggő káros gyakorlataira, erőfölénnyel visszaélő magatartására. A platformjogszabályok számos rendelkezése – mivel a személyes adatok kezelésének piaci versenyt érintő szabályozási igénye hívta életre – a GDPR-ból nőtt ki. Ebben az értelemben a GDPR a lex generalis, a többi pedig lex speciális jelleggel kiegészíti, pontosítja azt a személyes adatok felhasználásának további szigorításával.

A DMA rendelkezései az online hirdetésekben a személyesadat-felhasználás korlátozásával és a kapcsolódó kötelezettségekkel, a Data Act rendelkezései az IoT-termékek és a kapcsolódó szolgáltatások adatainak megosztási lehetőségével a kapuőrök tisztességes piaci magatartását célozza, ezzel a felhasználók számára biztonságosabb online teret képeznek, az európai digitális vállalkozások számára egyenlő versenyfeltételeket teremtenek, ezzel együtt előmozdíthatják a piacok élénkülését. Ha az adatokat jól használják fel, akkor elkezdődhet az elszakadás az amerikai platformoktól, csökken az adatfüggőség tőlük, az európai adatvagyon is itt marad, és itt kerül felhasználásra.

⁶⁷⁷ COM(2021) 713 final. A Bizottság közleménye az Európai Parlamentnek, a Tanácsnak, az Európai Gazdasági és Szociális Bizottságnak és a Régiók Bizottságának: Az új kihívásokra felkészült versenypolitika. Brüsszel, 2021. 11. 18. 17.

VI. FEJEZET: A FOGYASZTÓVÉDELEM ESZKÖZRENDSZERE – A SZEMÉLYES ADATOKKAL ÖSSZEFÜGGÉSBEN

A digitális piacok – a személyes adatok gyűjtése és felhasználása tekintetében – egyszerre két különböző piaci kudartól szenvednek: a platformok piaci erejétől, valamint az információs és magatartási, viselkedési problémáktól.⁶⁷⁸ Az előző fejezet ennek versenyjogi vonatkozásait tárta fel; e fejezet szempontjából az információs problémák értelmezése fontos. Az információs aszimmetria a fogyasztói döntések befolyásolásához, a fogyasztók manipulálásához vezethet, kordában tartását szolgálja a fogyasztóvédelem eszköztársa, így biztosítva a fogyasztók védelmét. A dolgozat egésze szempontjából hangsúlyos kérdésként merül föl, hogy a személyes adatokkal összefüggésben az EU fogyasztóvédelmi tárgyú jogalkotási aktusai mennyiben képesek reagálni a szolgáltatók, az online platformok okozta kihívásokra, rendelkezéseik adaptálhatók-e a digitális környezet generálta új helyzetekre. Mindezek előtt az adatvédelem, a versenyjog és a fogyasztóvédelmi jog gyakorlati összefonódására világítok rá, néhány jögesettel érvelve az összefüggésük mellett.

1. Adatvédelem, piaci verseny és fogyasztóvédelem, valamint ezek uniós szabályozásának összefonódása

A fogyasztóvédelmet a maastrichti szerződés (1992) emelte a közösségi politikák közé.⁶⁷⁹ Ez az irány folytatódott az amszterdami szerződésben (1999), amely rögzítette, hogy a közösségnek hozzá kell járulnia a fogyasztók gazdasági érdekeinek védelméhez, a fogyasztóvédelmi követelményeket pedig figyelembe kell venni az egyéb közösségi politikák meghatározásakor és végrehajtásakor,⁶⁸⁰ majd a Chartában is megerősítésre került, hogy az EU politikáiban biztosítani kell a fogyasztók védelmének magas szintjét.⁶⁸¹ A hangzatos célok és a különféle dokumentumok készítése⁶⁸² ellenére a fogyasztóvédelem nem tartozik a legerősebb uniós politikák közé.⁶⁸³ Ez leginkább azzal magyarázható, hogy a fogyasztóvédelem nem önálló jogág, hanem horizontálisan kapcsolódik a többi közösségi politikához; valamint azzal, hogy – mivel a fogyasztóvédelmi jogszabályok alkotása az EU és a tagállamok megosztott

⁶⁷⁸ KERBER–SPECHT–RIEMENSCHNEIDER i. m. 21.

⁶⁷⁹ Maastrichti szerződés 3. cikk (1) bekezdés t) pont

⁶⁸⁰ Amszterdami szerződés 153. cikk (1)–(2) bekezdés

⁶⁸¹ Charta 38. cikk

⁶⁸² Európai fogyasztói stratégia, fogyasztóvédelmi politikai jelentések, három- és ötéves tervek, zöld könyv

⁶⁸³ TÓTH Tihamér: *Fogyasztóvédelmi közjog*. Egyetemi jegyzet és szöveggyűjtemény. Pécs, 2017. 18. <https://jak.ppke.hu/uploads/articles/12239/file/Fogyik%C3%B6zjogjegyzet%20-%20T%C3%B3th%20Tiham%C3%A9r.pdf> (letöltés: 2023. 01. 03.)

hatáskörébe⁶⁸⁴ tartozik – rendeletek helyett többnyire irányelvekkel igyekszik az EU a fogyasztóvédelmi céljait elérni. Mindezekből következően a fogyasztóvédelmi intézkedések széttagoltak, a fogyasztóvédelmi tárgyú jogszabályok nem alkotnak koherens és egységes rendszert. Ennek egyszerű példája az, hogy a fogyasztó fogalmát sem egységesen definiálják a vonatkozó jogszabályok.

Mivel a digitális piac egyik oldala a fogyasztók köre, ez fogyasztóvédelmi kérdéseket is felvet. A fogyasztóvédelem és a versenyjog metszéspontját vizsgálva, a jelenlegi struktúra szerint, az egyes fogyasztók védelme a fogyasztóvédelem feladata, a verseny folyamatának védelme a versenyjog feladata, ezáltal a versenyjog közvetve szolgálja a fogyasztók helyzetének, jólétének javulását, ami a verseny előnyeinek érzékelésén keresztül realizálódik;⁶⁸⁵ a fogyasztóvédelmi jog pedig közvetlenül. A fogyasztóvédelmi jogszabályoknak ott kell beavatkozni, ahol a fogyasztó már nem tud tájékozott döntést hozni önmaga, ebből következően a digitális piacokon akár a személyes adatokkal rendelkezés tekintetében is segítségre szorulhatnak az érintettek. Digitális környezetben az adatvédelem, a versenyjog és a fogyasztóvédelem még hangsúlyosabban fonódik össze. A közös eredő a célban rejlik: a fogyasztói jólét különböző mértékű és tartalmú támogatása.

1.1. Jogesetek az adatvédelem, a versenyjog és a fogyasztóvédelem metszetében

Ahogy a Facebook kontra Bundeskartellamt ügy, úgy az olasz Facebook-ügy szintén azt mutatja, hogy az adatkezelés és következményei mindhárom területet érintik, de az utóbbi ügyben csak fogyasztóvédelmi vizsgálat és elmarasztalás történt. Az AGCM 2018-ban két bírságot szabott ki. Vizsgálata során megállapította, hogy a Facebook félrevezeti a fogyasztókat a szolgáltatása ingyenesnek feltüntetésével, másrészt a hozzájárulás tekintetében befolyásolja őket, akik ezért nem tudnak szabad és tájékozott döntést hozni a személyes adataikról rendelkezés során.⁶⁸⁶ Az AGCM-nek lehetősége lett volna – főleg a személyes adatok harmadik felekkel való megosztása kapcsán – versenyjogi alapon eljárást indítani, a piaci erőfölényt

⁶⁸⁴ EUMSZ 4. cikk (2) bekezdés f) pont

⁶⁸⁵ BENCSIK András: *A versenyjog szerepe a fogyasztói érdekek védelmében*. Jura 2012/2. 27.

⁶⁸⁶ Facebook fined 10 million Euros by the ICA for unfair commercial practices for using its subscribers' data for commercial purposes. Sajtóközlemény, 2018. 12. 07. [AGCM - Autorita' Garante della Concorrenza e del Mercato](#) (letöltés: 2024. 02. 02.). Magyarországon 2019-ben a GVH 1,2 milliárd Ft-os bírságot szabott ki a Facebookra a fogyasztókkal szembeni tisztességtelen kereskedelmi gyakorlat tilalmának megsértése miatt (ingyenesnek hirdette szolgáltatását, de a felhasználók adataikkal és aktivitásukkal fizettek a szolgáltatás igénybevételéért, s ezzel üzleti hasznot hajtottak a Facebooknak). Vj-85/2016/189. A Fővárosi Törvényszék a 105.K.701.043/2020/14. számú ítéletével a GVH határozatát megsemmisítette, majd a GVH a fogyasztóvédelmi ügyben hozott határozat jogszerűsége vizsgálatát kérte, amelynek során a Kúria a Fővárosi Törvényszék ítéletét hatályában fenntartotta. Kfv.II.37.243/2021/11.

bizonyítani és valószínűleg az ezzel való visszaélést megállapítani, és meg is tehette volna, mert integrált hatóságként versenyhatósági és fogyasztóvédelmi feladatokat is ellát (szemben a Bundeskartellamtal, amely csak versenyhatóság), mégis fogyasztóvédelmi hatáskörében járt el, és a jogsértést agresszív kereskedelmi gyakorlatként értékelte. Szabályozási dilemmával néztek szembe, végül a versenyjogi vizsgálat nehézségei, időigényessége és a nagyobb bírság lehetősége helyett az egyszerűbb, de szinte biztos utat választották, amelynél a bírság lényegesen alacsonyabb, kevésbé elrettentő, és nem ad lehetőséget a problémák magatartási kötelezettségvállaláson keresztül történő kezelésére, így módon az is kérdéses, hogy rábírja-e a vállalatot a jogsértő magatartás befejezésére.

Egy németországi gyógyszerész a német versenytörvény⁶⁸⁷ alapján – mely szerint a fogyasztókat is meg kell védeni a tisztességtelen kereskedelmi gyakorlatoktól – perelte be a versenytársát, mert az a kizárólag gyógyszertárban forgalmazható gyógyszereket az Amazon online platformon értékesíti, feltételezhetően a fogyasztók GDPR szerinti hozzájárulása nélkül. Az EUB ítélete szerint a gyógyszerek online megrendelésekor megadott név, szállítási cím, a gyógyszerek személyre szabásához szükséges információk stb. a GDPR 9. cikk (1) bekezdése szerinti egészségügyi adatoknak minősülnek; valamint a GDPR 82. cikk (1) bekezdése alapján kártérítésre jogosult minden olyan személy, aki vagyoni vagy nem vagyoni kárt szenvedett e rendelet megsértésének következményeként, és a kár közvetetten is elszenvedhető, még akkor is, ha a károsult fél nem az adatalany.⁶⁸⁸ Ez az ügy is azt erősíti, hogy a személyes adatok védelmére vonatkozó rendelkezések megsértése egyúttal a fogyasztóvédelmi vonatkozású szabályok, azaz a tisztességtelen kereskedelmi gyakorlatok tilalma megsértésének lehetőségét is hordozza, valamint az erőfölénnyel való visszaélés fennállásának értékelésére is hatással lehet, éppúgy, mint a Facebook kontra Bundeskartellamt ügyben láttuk.

A szabályozási dilemma feloldására egyelőre csak elméleti szintű megközelítések léteznek. Az európai adatvédelmi biztos már 2014-ben kimutatta a kapcsolódási pontokat az adatvédelem, a versenyjog és a fogyasztóvédelem között, és a szabályozók közötti szorosabb koordinációt és termékeny együttműködést javasolt.⁶⁸⁹ Emellett digitális információs központ, ún. digitális elszámolóház (Digital Clearinghouse) létrehozását javasolta, amely az e

⁶⁸⁷ Gesetz gegen den unlauteren Wettbewerb (tisztességtelen verseny tilalmáról szóló törvény (UWG) 3. § (1) bekezdés és 3a. §: A tisztességtelen kereskedelmi gyakorlatok alkalmazása jogellenes, és tisztességtelenül jár el, aki a piaci magatartás gazdasági szereplők érdekében történő szabályozására is irányuló valamely jogszabályt megsért, ha a jogsértés alkalmas arra, hogy érzékelhetően csorbítsa a fogyasztók, a piac egyéb résztvevői vagy a versenytársak érdekeit.

⁶⁸⁸ ECLI:EU:C:2024:846. A Bíróság ítélete (nagytanács) a C-21/23. sz. ügyben (gyógyszerek forgalmazása online platformon), 2024. október 4. 95. pont és 55. pont

⁶⁸⁹ 2014/C 225/07.

területeken működő szervek összefogásával törekszik kialakítani a digitális gazdaságra vonatkozóan az együttműködési formákat. A szervezet 2017-től működik, és jelenleg a szabályozáson átívelő együttműködés jövőjéről egyeztetnek.⁶⁹⁰ Hatékonyságát azonban megkérdőjelezi az, hogy például az AGCM és a Bundeskartellamt között – noha hasonló helyzetet kellett értelmezniük és arról dönteniük – semmilyen együttműködés nem volt, pedig a digitális elszámolóház koordinálhatta volna.⁶⁹¹ A Bizottság a GDPR alkalmazását értékelő első közleményében szintén elismerte az adatvédelem szoros kapcsolatát a fogyasztóvédelemmel és a versennyel; az EDPB pedig kifejezte együttműködési szándékát az érintett szabályozókkal.⁶⁹² A folyamat jelenleg ott tart, hogy az EU még mindig csak a szorosabb együttműködés és az új megközelítés szükségességét rögzíti a három hatóság között,⁶⁹³ érdemi előrelépés azonban nem történt.

2. A fogyasztóvédelmi eszközrendszer a fogyasztók aszimmetrikus helyzetének kezelésére

A fogyasztóvédelem eszközrendszerének – összefüggésben a személyes adatok gyűjtésével és kezelésével – több összetevője van. A tájékoztatási kötelezettségek és a kapcsolódó átláthatósági követelmények szabályozását a CR-irányelv, a GDPR és a DSA tartalmazza, utóbbi kettő hangsúlyt helyez a kockázatok mérséklésére is. A szerződési feltételekkel három irányelv is foglalkozik: a UCT-, a CR- és a DCS-irányelv. A tisztességtelen kereskedelmi gyakorlatok a UCP-irányelv, a sötét megoldások elleni fellépés szintén a UCP-irányelv és a DSA hatálya alá tartozik. A fogyasztóvédelmi eszközök fontos eleme a gyermekek védelme, erre vonatkozó rendelkezéseket tartalmaz a GDPR, a DSA és a UCP-irányelv is. Ide tartoznak a fogyasztók számára utólagos megoldást kínáló jogorvoslati lehetőségek is, ezekkel részletesen nem foglalkozom, annyit azonban érdemes megjegyezni, hogy egyes platformok – mint „új versenytársak az igazságszolgáltatás piacán” – azon iparkodnak, hogy „a saját szolgáltatásaikkal kapcsolatos vitás kérdésekre hatékony és gyors megoldást biztosítsanak, elsősorban saját platformjaikon keresztül intézhető vitarendezési eljárásokkal” (pl. Alibaba).⁶⁹⁴

⁶⁹⁰ EDPS.EUROPA.EU: *Big Data & Digital Clearinghouse*. [Big Data & Digital Clearinghouse | European Data Protection Supervisor](#) (letöltés: 2024. 10. 20.)

⁶⁹¹ Marco BOTTA – Klaus WIEDEMANN: 'The Interaction of EU Competition, Consumer, and Data Protection Law in the Digital Economy: The Regulatory Dilemma in the Facebook Odyssey.' *Antitrust Bulletin* 2019/3. 428–446. V. How to Solve the „Regulatory Dilemma”? <https://doi.org/10.1177/0003603X19863590> (letöltés: 2022. 10. 22.).

⁶⁹² COM(2020) 264 final

⁶⁹³ *Fitness Check* i. m. 347–348.

⁶⁹⁴ OSZTOVITS András: *A technológia hálójában – a magánjogi jogérvényesítés jelene és lehetséges jövője*. In: ZÖDI Zsolt (szerk.): *Jogi technológiák: Digitális jogalkalmazás*. Bp., Ludovika Egyetemi Kiadó, 2022. 289. A szerző gondolatmenete szerint az automatizálás, az információs technológia használata az igazságszolgáltatás

A felsorolt uniós jogforrások megalkotásuk idején tipikusan egy-egy fogyasztóvédelmi eszköz tekintetében igyekeztek ellensúlyozni az offline piactereken jelen lévő információs aszimmetriát. A digitális környezet, a platformok felemelkedése elvezetett ahhoz a felismeréshez, hogy a személyes adatok nagyarányú gyűjtése és kezelése a fogyasztók szempontjából is jogalkotói beavatkozást kíván, és 2019-ben az omnibusz irányelv módosította a CR-, a UCT- és a UCP-irányelvet, ill. ugyanekkor keletkezett a DCS-irányelv, majd 2022-ben a DSA, amely a digitális szolgáltatások használatával összefüggésben védi a fogyasztókat.

2.1. Kockázatkezelés, átláthatóság, kiskorúak védelme – a DSA a fogyasztók védelmében

A DSA hasonló megfontolásból született, mint ikertestvére, a DMA, de ennek tárgyát nem a digitális piacok, hanem a közvetítő szolgáltatások képezik, így az árukat, a fogyasztókat, a szolgáltatásokat vagy a tartalmakat – felület biztosításával – közvetítő digitális szolgáltatások. A DSA, célja szerint, a belső piac megfelelő működéséhez kíván hozzájárulni a biztonságos, kiszámítható és megbízható online környezetre vonatkozó szabályok meghatározásával, amelyek egyrészt az innovációt segítik, másrészt az alapvető jogokra, köztük a fogyasztók védelmére fókuszálnak.⁶⁹⁵ A DSA a földrajzi hatályt a közvetítő szolgáltatók letelepedési helyétől függetlenül határozza meg, helyette az igénybe vevők EU-hoz kötöttségét veszi alapul,⁶⁹⁶ vagyis a hatálya alá tartozik – legalább néhány kötelezettség tekintetében – minden digitális szolgáltató, mérettől és forgalomtól függetlenül, aki/amely az EU területén közvetítő szolgáltatást végez. Azért terjed ki a DSA hatálya minden közvetítő szolgáltatóra, mert a szolgáltatások használata kockázatokat hordoz, ami erősen igényli a fogyasztóvédelmi szempontok érvényesítését.

A klasszikus fogyasztóvédelmi jogszabályok a tranzakcióban részt vevő kötelezetteket és védendő feleket aszerint különítik el, hogy kereskedelmi vagy nem kereskedelmi célból járnak-e el, és eltekintenek mind a vállalkozás méretétől, mind a személyes jellemzőktől,⁶⁹⁷ előbbiek a kereskedők, utóbbiak a fogyasztók. Ehhez képest a DSA által védendő felek a

szükségszerű megújulásához is vezethetne „a jól tipizálható ügyek, jogkérdések esetén,” példaként említve a kínai online bíróságokat, amelyek hatáskörébe nagyrészt a fogyasztói jogviszonnyal összefüggő jogviták (pl. internetes vásárlás, valamint az ebből eredő termékfelelősségi kérdések) elbírálása tartozik. OSZTOVITS i. m. 292–300.

⁶⁹⁵ DSA 1. cikk (1) bekezdés

⁶⁹⁶ DSA 2. cikk (1) bekezdés

⁶⁹⁷ DE ELIZALDE: F. *Fragmenting Consumer Law Through Data Protection and Digital Market Regulations: The DMA, the DSA, the GDPR, and EU Consumer Law*. Journal of Consumer Policy 2025/48. 365. <https://doi.org/10.1007/s10603-025-09584-3> (letöltés: 2025. 03. 02.)

szolgáltatást igénybe vevők – fogyasztók,⁶⁹⁸ üzleti felhasználók, egyéb felhasználók, online platformok és online keresőmotorok aktív igénybe vevői –, vagyis bármely természetes vagy jogi személyek, akik/amelyek a szolgáltatást az információkeresés vagy annak hozzáférhetővé tétele céljából veszik igénybe.⁶⁹⁹ Más fogyasztóvédelmi célú jogszabályokhoz képest a fogyasztói, kedvezményezetti kört kibővíti egyrészt a jogi személyekkel, másrészt az említett cél mentén; amivel felborítja a korábbi szabályozás logikáját, szétzúrodottá teszi,⁷⁰⁰ és befolyásolja a fogyasztóvédelmi jog horizontális eszközeit, így a UCP- és a UCT-irányelvet.⁷⁰¹

A DSA kötelezettjeinek sorában szerepelnek a kereskedők – s fogalmát is a fogyasztóvédelmi jogszabályokkal azonosan határozza meg⁷⁰² –, de nem ők képezik a szabályozás célpontjait,⁷⁰³ hanem a közvetítő szolgáltatók. A közvetítő szolgáltatások az online térhez kötöttek, és az információs társadalom szolgáltatásai: az egyszerű továbbítás, a gyorsítótárazás vagy a tárhelyszolgáltatás⁷⁰⁴ tartoznak a körükbe. A DSA-ben a közvetítő szolgáltatókat a méretük és a szolgáltatásaik jellegének ötvözete szerint rendszerezi a jogalkotó, és differenciáltan állapít meg kötelezettségeket valamennyi közvetítő szolgáltató számára, a tárhelyszolgáltatók számára, az online platformok számára; továbbá külön kategóriába sorolja az online óriásplatformot üzemeltető szolgáltatókat (VLOP) és a nagyon népszerű online keresőprogramot üzemeltető szolgáltatókat (VLOSE) is.

Amennyiben a szolgáltatók több különböző kategóriába is tartoznak, az ilyen szolgáltatásokra vonatkozó valamennyi kötelezettség vonatkozik rájuk. A jogalkotó azért nem alkot homogén kategóriákat, mert egyrészt – a DSA célja szerint – a szolgáltatások használatához kapcsolódó kockázatokat veszi alapul; másrészt a kisebb online szolgáltatók innovációjának és fejlődésének is teret kíván adni, ezért ezekre kevesebb kötelezettséget telepít.

⁶⁹⁸ Hohmann Balázs érvelése szerint az igénybe vevő akkor válik tényleges fogyasztóvá, ha a szolgáltatásért árat fizet. Az ingyenes szolgáltatások tekintetében nincs díjfizetés, azonban az internethasználatért van, ezért közvetett fogyasztói jogviszony keletkezik. HOHMANN i. m. 79.

⁶⁹⁹ DSA (2) preambulumbekzdés, 3. cikk p)–q) pont, 3. cikk b) pont

⁷⁰⁰ DE ELIZALDE i. m. 370.

⁷⁰¹ Hans-W. MICKLITZ: *Dissolution of EU consumer law through fragmentation and privatisation*. In Natali HELBERGER et al.: *Digital fairness for consumers*. 2024. 72.

⁷⁰² DSA 3. cikk f) pont. Az online platformot üzemeltető szolgáltatók egyes kötelezettségeinek szempontjából van szerepük a kereskedőknek: DSA III. fejezet 4. szakasz: Az olyan online platformot üzemeltető szolgáltatókra alkalmazandó egyéb rendelkezések, amelyek lehetővé teszik a fogyasztók számára, hogy távollevők közötti szerződéseket kössenek a kereskedőkkel.

⁷⁰³ DE ELIZALDE i. m. 370.

⁷⁰⁴ A fogalom meghatározások a DSA 3. cikk g) pontja, a példák a DSA (29) preambulumbekzdése alapján: Egyszerű továbbítás: az igénybe vevő által küldött információnak hírközlő hálózaton keresztül történő továbbítása vagy ehhez hozzáférés biztosítása; pl. internetkapcsolódási pontok, DNS-szolgáltatások és -átalakítók, doménnév-nyilvántartások. Gyorsítótárazás: az egyszerű továbbítás együtt jár az információ automatikus, közbenső és átmeneti tárolásával, és azzal a kizárólagos céllal hajtják végre, hogy az információ későbbi továbbítását a szolgáltatás más igénybe vevői számára hatékonyabbá tegyék; pl. tartalomszolgáltató hálózatok, fordított proxyk. Tárhelyszolgáltatás: a szolgáltatás igénybe vevője által küldött információ tárolása; pl. felhőszolgáltatás, internetes tárhelyszolgáltatás, információk és tartalmak online megosztását lehetővé tevő szolgáltatások.

Minél nagyobb azonban egy közvetítő szolgáltató, annál több kockázatot hordozhat a szolgáltatása használata, és annál nagyobb a szolgáltató felelőssége. A kockázatokból ered a tartalommoderálási és az átláthatósági kötelezettség, valamint a profilalkotáson alapuló célzott reklámozás tilalma a kiskorúak védelme érdekében. A gondossági kötelezettségek előírása azt is jelenti, hogy a DSA „egyfajta társszabályozás is abban az értelemben, hogy az EU elismeri az online platformok [...] szabályozói képességét, és ezt a képességet szabályozza, ami [...] a kereskedőkkel szembeni fogyasztóvédelmi elvárások kikényszerítésének fokozására” teszi őket alkalmassá.⁷⁰⁵ A jogalkotó e gondossági kötelezettségek egymásra épülő rendszerével – ahogy Hajnal Zsolt megállapította – szabályozási ökoszisztémát alakított ki.⁷⁰⁶

2.1.1. A DSA által támasztott követelmények

A tartalommoderálás követelménye szerint valamennyi közvetítő szolgáltató kötelessége, hogy felismerje, észlelje, azonosítsa és kezelje a szolgáltatás igénybe vevője által közzétett jogellenes tartalmat. A kezelés során az ilyen tartalom elérhetőségét, láthatóságát és hozzáférhetőségét érintő intézkedéseket (pl. annak hátrасorolása, a hozzáférés megszüntetése); vagy a szolgáltatás igénybe vevője általi információközlés lehetőségét érintő intézkedéseket (pl. fiókja megszüntetése vagy felfüggesztése) kell hoznia.⁷⁰⁷ Jogellenes tartalomnak tekintendők az olyan információk, amelyek az alkalmazandó jog értelmében vagy önmagukban is jogellenesek, ilyen a gyűlöletbeszéd vagy a terrorista tartalom; vagy jogellenes tevékenységhez kapcsolódnak, például gyermekek szexuális bántalmazását ábrázoló képek megosztása, magánjellegű képek beleegyezés nélküli megosztása stb.⁷⁰⁸ A szolgáltatás igénybe vevőjét tájékoztatni kell a szerződési feltételekben az általa adott információkra vonatkozó korlátozásokról, ideértve a tartalommoderálás szabályait, eljárásait, intézkedéseit és eszközeit (az algoritmikus döntéshozatalt és az emberi felülvizsgálatot is), valamint a panaszkezelési rendszerükre vonatkozó információkat.⁷⁰⁹

Az átláthatóság követelményének konkrét jogintézményei közül a DSA minden közvetítő szolgáltató számára kötelezettségként írja elő, hogy legalább évente egyszer – géppel olvasható formátumban és könnyen hozzáférhető módon világos, jól érthető –

⁷⁰⁵ TÓTH András: *A Digital Services Act és az EU fogyasztóvédelmi joga*. KözigazgatásTudomány, 2023/2. 25–26. <https://doi.org/10.54200/kt.v3i2.67> (letöltés: 2024. 02. 02.)

⁷⁰⁶ HAJNAL Zsolt: *A digitális szolgáltatásokról szóló rendelet közvetítő szolgáltatókra vonatkozó új kötelezettségeiről, felelősségéről*. In: NEMESSÁNYI Zoltán (szerk.): *Nemzetközi magánjogi évkönyv*. 2024. Bp., Orac Kiadó, 2024. 159.

⁷⁰⁷ DSA 3. cikk t) pont

⁷⁰⁸ DSA (12) preambulumbekzdés

⁷⁰⁹ DSA 14. cikk (1) bekezdés

transzparenciajelentést tegyen közzé az általa végzett tartalommoderálásról, a döntéseiről. E jelentések azokat az illegális tartalmakkal kapcsolatos statisztikai összegzéseket tartalmazzák, amelyek felszínre kerültek, és intézkedést vontak maguk után (végzések száma, jogellenes tartalom típusa, panaszok száma, intézkedések stb.).⁷¹⁰

A DSA fogalomhasználatában a hirdetés – üzenet népszerűsítésére szolgáló információ, amelyért ellentételezéssel fizettek – nemcsak a kereskedelmi célú üzeneteket foglalja magában,⁷¹¹ hanem a dezinformáció, a jogellenes vagy egyéb módon káros tartalmak közzétételét is, vagyis a tág meghatározás a tartalommoderálás követelményéből ered.⁷¹² A hirdetések átláthatóságával kapcsolatban az online platformot üzemeltető szolgáltatóknak tömören, egyértelműen és valós időben – akár szabványokkal támogatottan megjelenítve⁷¹³ – fel kell tüntetni a szolgáltatások igénybe vevői számára azt, hogy adott információ hirdetésnek minősül; a hirdetés megbízójára vonatkozó információkat, valamint a finanszírozóját; a megcélzott igénybe vevők meghatározására szolgáló főbb paramétereket, amelyek által megértik, miért látják az adott hirdetést; valamint e paraméterek módosítási lehetőségeit.⁷¹⁴ Utóbbi kettő a kérértlen hirdetésekkel szemben nyújt védelmet a felhasználók számára. Az online platformokra telepített kötelezettségek célja az, hogy a „harmadik felek a fogyasztóvédelmi elvárásoknak jobban megfelelhessenek,” ill. hogy a felületükön „hirdetők azonosításához és felelősségre vonásukhoz [...] szükséges adatok rendelkezésre álljanak.”⁷¹⁵ Az online óriásplatformot, ill. nagyon népszerű online keresőprogramot üzemeltető szolgáltatók számára további átláthatósági kötelezettséget állapít meg: nyilvánosan hozzáférhetővé kell tenniük a felületükön megjelenített összes hirdetés adattárát a hirdetés megjelenítésének teljes időtartama alatt, majd még egy évig, gondoskodva arról, hogy az adattár ne tartalmazzon a szolgáltatás olyan igénybe vevőinek személyes adatait, akik számára a hirdetés megjelenítésre került.⁷¹⁶ Az elszámoltathatóság elve alapján olyan rendszereket is működtetniük kell, amelyek segítségével a felhasználók fellebbezhetnek a szolgáltató őket érintő, bármilyen korlátozást jelentő döntése ellen, és az ilyen döntést indokolni kell.⁷¹⁷

⁷¹⁰ DSA 15. cikk

⁷¹¹ DSA 3. cikk r) pont

⁷¹² MICKLITZ *i. m.* 75.

⁷¹³ DSA 44. cikk h) pont

⁷¹⁴ DSA 26. cikk (1) bekezdés

⁷¹⁵ TÓTH (2023) *i. m.* 30–31.

⁷¹⁶ DSA 39. cikk

⁷¹⁷ DSA 17. cikk

2.1.2. A GDPR és a DSA rendelkezéseinek összevetése a személyes adatok tekintetében

A GDPR és a DSA a biztonságosabb online környezet biztosítására törekszik, de más-más szempontból közelít céljához. A GDPR – mint *lex generalis* – keretjelleggel szabályozza azt, hogy a vállalatok hogyan gyűjthetik és kezelhetik a személyes adatokat, valamint szabályozza az érintettek ellenőrzési és rendelkezési jogait az adataikkal kapcsolatban, például hozzáférhetnek adataikhoz, helyesbíthetik vagy törölthetik azokat. Erre az adatvédelmi keretrendszerre épít a *lex specialis*-nak tekinthető DSA, amely az online szolgáltatások használatához kapcsolódó kockázatokat szabályozza. Az online környezetben a felhasználók ki vannak téve annak, hogy jogellenes tartalmakkal, dezinformációkkal,⁷¹⁸ valamint a szolgáltatók tisztességtelen gyakorlataival szembesüljenek a szolgáltatások használata során, az ezekhez kapcsolódó kockázatok kezelését a jogalkotó a közvetítő szolgáltatók felelősségi körébe utalja.

A kockázatkezelést illetően a GDPR és a DSA is rendelkezik. Előbbi hatásvizsgálatot és a kockázatok kezelését célzó intézkedések tervezését írja elő arra az esetre vonatkozóan, ha a tervezett adatkezelés magas kockázattal jár a természetes személyek jogaira és szabadságaira nézve.⁷¹⁹ Az adatvédelmi hatásvizsgálattal kapcsolatos feladatokat a GDPR az adatkezelőre ruházza. A DSA alapján az elszámoltathatóság elvét tekintve az online óriásplatformoknak és a nagyon népszerű online keresőprogramoknak szintén rendszeresen azonosítaniuk, elemezniük és értékelniük kell a szolgáltatásaikhoz kapcsolódó rendszerszintű kockázatokat, beleértve az algoritmikus rendszerek jelentette kockázatokat is, és e kockázatok mérséklésére intézkedéseket kell tenniük. A rendszerszintű kockázatok fogalmát nem határozza meg a DSA, de felsorolja azok alaptípusait, ezzel pótolva a hiányzó definíciót. A rendszerszintű kockázatok négy kategóriába sorolhatók: a) a jogellenes tartalom terjesztése; b) a szolgáltatások hatása a társadalmi folyamatokra (pl. a választásokra, közbiztonságra vonatkozó szándékos manipuláció lehetősége); c) a Chartában lefektetett alapvető jogokra gyakorolt hatás; d) az emberrel mint biológiai lényvel összefüggésben a negatív hatások (a közegészséggel kapcsolatban, valamint a személyek testi és szellemi jóllétére gyakorolt negatív következmények), amelyek főleg az online óriásplatformok és a nagyon népszerű online keresőprogramok kialakításából,

⁷¹⁸ A DSA nem definiálja. Köznyelvi jelentése: félretájékoztatás, ebből kiindulva határozta meg a Bizottság is: igazolhatóan hamis vagy félrevezető információ, amelyet gazdasági haszonszerzés vagy szándékos megtévesztés céljából terjesztenek, és amely kárt okozhat a közérdeknek azáltal, hogy fenyegeti a demokratikus döntéshozatali folyamatokat és a közjavakat (pl. az uniós polgárok egészségét, a környezet védelmét). A dezinformáció visszaszorítását célzó gyakorlati kódex, 2018. 1., <https://digital-strategy.ec.europa.eu/hu/library/2018-code-practice-disinformation> (letöltés: 2022. 12. 22.).

⁷¹⁹ GDPR 35. cikk (1) és (7) bekezdés

működéséből vagy használatából erednek. A Charta által védett alapvető jogokat nevesíti is a DSA a rendszerszintű kockázatok elemzésének fontos szempontjaiként, ezek között említve a magán- és a családi élet tiszteletben tartásához, a személyes adatok védelméhez, a gyermekek jogainak védelméhez való alapvető jogot.⁷²⁰

A kockázatok kezelésével kapcsolatban a két rendeletet összevetve azt látjuk, hogy a GDPR esetében sokkal szélesebb az adatkezelők feladatköre és felelőssége is, hiszen ők dolgozzák ki a szervezetükre szabott szempontokat, s ebben csak az iránymutatások, a magatartási kódexek és az adatvédelmi tisztviselők segítik őket. A DSA azonban számottevően csökkenti a rendelet címzettjeinek mérlegelési mozgásterét,⁷²¹ hiszen meghatározza a rendszerszintű kockázatok négy kategóriáját, valamint azok befolyásoló tényezőit, többek között az ajánlórendszereik és más algoritmikus rendszerük kialakítását; a tartalommoderálási rendszereiket vagy a hirdetések kiválasztását és megjelenítését végző rendszereket,⁷²² tehát a mérlegelésnek itt már nem lehet helye.

Konkrét rendelkezéseik tekintetében is találunk közös pontokat a GDPR és a DSA között. A GDPR – néhány kivételtől eltekintve, például ha az adatkezelés az érintett hozzájárulása alapján történik – alapvetően tiltja a faji, etnikai, politikai, vallási vagy világnézeti jellemzőkre vagy szakszervezeti tagságra utaló személyes adatok, valamint a genetikai és biometrikus adatok, az egészségügyi adatok és a szexuális életre, irányultságra vonatkozó személyes adatok kezelését.⁷²³ Ennek oka az, hogy ezen adatok kezelésének körülményei nagy kockázatot jelenthetnek az alapvető jogok és szabadságok tekintetében. A DSA ettől erősebb rendelkezést tartalmaz. Az online platformot üzemeltető szolgáltatók nem jeleníthetnek meg profilalkotáson alapuló hirdetéseket a felhasználók – előbb felsorolt – érzékeny, különleges adatai felhasználásával. Itt a DSA két tekintetben is visszautal a GDPR-ra: egyrészt a profilalkotás fogalmával, másrészt a személyes adatok különleges kategóriáinak meghatározásával.⁷²⁴ A profilalkotáson alapuló online hirdetésekben a személyes adatok különleges kategóriáinak felhasználási tilalma hátterében az áll, hogy negatív hatással járhat, ha a szolgáltatás igénybe vevői az érdeklődésüknek megfelelően olyan célzott hirdetéseket látnak, amelyek a gyenge pontjaikat használják ki. Különösen így van ez, ha a manipulatív

⁷²⁰ DSA 34. és 35. cikk

⁷²¹ MEZEI Kitti – TRÄGER Anikó: *Kockázatok és reziliencia az online platformok és a mesterséges intelligencia európai uniós szabályozásában*. MTA Law Working Papers 2024/1. 8. <https://jog.tk.hun-ren.hu/mtalwp/kockazatok-es-reziliencia-az-online-platformok-es-a-mesterseges-intelligencia-europai-unios-szabalyozasaban> (letöltés: 2024. 09. 11.)

⁷²² DSA 34. cikk (2) bekezdés

⁷²³ GDPR 9. cikk (1) bekezdés

⁷²⁴ DSA 26. cikk (3) bekezdés

technikák nemcsak egyes személyeket, hanem egész csoportokat érintenek, ugyanis erősíthetik a társadalmi károkozást, például dezinformációs kampányokhoz hozzájárulva. Az online platformok különösen érzékeny környezetet jelentenek az ilyen gyakorlatok tekintetében, és nagyobb társadalmi kockázattal járnak.⁷²⁵

A GDPR és a DSA érintkezik a kiskorúak védelmének kötelezettsége tekintetében is. A GDPR kiemeli, hogy a gyermekek személyes adatai különös védelmet érdemelnek, főleg abban az esetben, ha azokat marketingcélra vagy felhasználói profilok létrehozására használják,⁷²⁶ konkrétan azonban nem tiltja sem a gyermekeket célzó reklámozást, sem a profilalkotást velük kapcsolatban, ami azt jelenti, hogy a gyermekekre irányuló és profilalkotáson alapuló célzott reklámozás – a DSA hatályba lépése előtt – megengedett volt. A gyermekek magánéletének védelmét és biztonságát szolgálja az, hogy a DSA az online platformot üzemeltető szolgáltatóknak megtiltja, hogy a szolgáltatást igénybe vevők adatait felhasználó, profilalkotáson alapuló célzott hirdetéseket jelenítsenek meg, „ha kellő bizonyossággal tudatában vannak annak, hogy a szolgáltatás igénybe vevője kiskorú.”⁷²⁷ E tilalomból következően a platformszolgáltatóknak két feladattömböt kell megoldaniuk. Egyrészt meg kell győződniük arról, hogy a szolgáltatásaik igénybe vevője kiskorú-e, vagy sem; másrészt újra kell tervezniük szolgáltatásaikat, beleértve az interfészeket, az ajánlórendszereket.

A szolgáltató akkor győződhet meg kellő bizonyossággal az életkoráról, ha más célból már kezeli a szolgáltatás igénybe vevőinek életkorát tartalmazó személyes adatait.⁷²⁸ Más esetekben nem kérdezhetnek rá az életkorra, mert ez ellentétes az adattakarékosság elvével,⁷²⁹ s azzal járna, hogy még több személyes adatot kezelnének. E problémára kínál megoldást az euConsent,⁷³⁰ amely 2024 áprilisában bejelentést tett az – életkor-ellenőrzést, ill. a szülői felügyeletet biztosító – AgeAware alkalmazásról. Miután a felhasználó egyszer elvégezte az ellenőrzést, a digitális aláírással hitelesített, interoperábilis és anonimizált tokent az eszközére letöltheti, így az automatikusan választ ad az életkorra rákérdező további webhelyek számára.

Az online platformot üzemeltető szolgáltatók úgy tudnak megfelelni a DSA profilalkotáson alapuló célzott hirdetések tilalma rendelkezésének, ha az életkor megállapításán túl újratervezik a szoftvereiket és alkalmazásaikat is – a DSA szóhasználatával: az online interfészeket – oly módon, hogy azok már alapértelmezés szerint garantálják a magánélet

⁷²⁵ DSA (69) preambulumbekkezdés

⁷²⁶ GDPR (38) preambulumbekkezdés

⁷²⁷ DSA 28. cikk (1)–(3) bekezdés

⁷²⁸ DSA (71) preambulumbekkezdés

⁷²⁹ GDPR 5. cikk (1) bekezdés c) pont

⁷³⁰ EUCONSENT.EU i. m.

védelmét (ne legyen olyan interfész, amely függő viselkedésformát ösztönözhet vagy eredményezhet); vagy részt vesznek a kiskorúak védelmét szolgáló magatartási kódexekben.⁷³¹ Utóbbival kapcsolatban a Bizottság – összhangban a GDPR-ral – segíti az olyan átfogó uniós magatartási kódex kidolgozását, amely az életkornak megfelelő tervezéssel foglalkozik, és amelynek kidolgozásába az ipart és a gyermekeket is bevonja.⁷³² 2025 derekára elkészültek azok az iránymutatások, amelyek a kiskorúak védelmének biztosítását könnyítik meg a DSA rendelkezéseivel összefüggésben. Az ajánlások – a kiskorúak fiókjainak alapértelmezés szerinti privát beállítása, a túlzott használathoz hozzájáruló alapértelmezett funkciók letiltása, a nyúlüreghatás kiküszöbölése, a függőséget okozó magatartás kialakulása és a manipulatív kereskedelmi gyakorlatok elleni védelem stb. – azt a célt szolgálják, hogy biztonságos online élményhez jussanak a gyermekek és a fiatalok.⁷³³ Az iránymutatások beépített megoldásokat javasolnak, amelyek erőteljesen képesek a kockázatokat csökkenteni, amire égető szükség is van, mert a Bizottság már több hivatalos eljárást indított arra vonatkozóan, hogy a platformok betartják-e a kiskorúak védelmével kapcsolatos DSA-előírásokat.⁷³⁴

Még ezektől az intézkedésektől is tovább megy az a 2024-es tanulmány, amely az uniós fogyasztóvédelmi jogszabályokat vizsgálta a digitális méltányosság szempontjából. Prioritásként egyrészt a kiskorúak védelmének és jogainak erősítését jelöli meg, másrészt az érzékeny adatok védelmét, és azt javasolja, hogy minden kereskedő számára, tehát nem csak az online platformokra vonatkozólag, meg kell tiltani mind a kiskorúak, mind a személyes adatok különleges kategóriái vonatkozásában a profilalkotáson alapuló célzott reklámozást.⁷³⁵ Véleményem szerint e kettős tilalom kiterjesztése valódi hatással bírna a legsérülékenyebb,

⁷³¹ DSA (71) preambulumbekkezdés

⁷³² COM(2022) 212 final. A Bizottság közleménye az Európai Parlamentnek, a Tanácsnak, az Európai Gazdasági és Szociális Bizottságnak és a Régiók Bizottságának: Digitális évtized a gyermekek és az ifjúság számára: a gyermekbarát internetre (BIK+) vonatkozó új európai stratégia. Brüsszel, 2022. 05. 11. 11.; European Commission: Special group on the EU Code of conduct on age-appropriate design. 2023. 09. 20. <https://digital-strategy.ec.europa.eu/en/policies/group-age-appropriate-design> (letöltés: 2024. 08. 04.). A csoport még csak egyszer ülésezett.

⁷³³ C/2025/5519. A Bizottság közleménye: Iránymutatás a kiskorúak magas szintű online magánéleti védelmének és biztonságának az (EU) 2022/2065 rendelet 28. cikkének (4) bekezdése értelmében történő biztosítását célzó intézkedésekről. Brüsszel, 2025. 10. 10.

⁷³⁴ Többek között 2024 februárjában a TikTok platform ellen (2024 májusában a Facebookot és az Instagramot üzemeltető Meta ellen is indult hivatalos eljárás). A vizsgálat egyik területe a nyúlüreghatásnak (rabbit hole effect) nevezett viselkedési függőség: a felhasználókat egy algoritmus segítségével olyan kapcsolódó, folyamatosan frissülő tartalommal látják el, amely könnyen mentális függőséghez vezet, akár káros tartalmakhoz kalauzsolva őket. 2024. áprilisban másik eljárás indult a TikTok Lite alkalmazásának spanyolországi és franciaországi – előzetes gondos felmérés és hatékony kockázatcsökkentő intézkedések meghozatala nélküli – bevezetése kapcsán, mert annak feladat- és jutalomprogramja kritikus hatással lehet a rendszerszintű kockázatokra, különösen a felhasználók mentális egészségére. A TikTok önként leállította a Lite bevezetését. ONLINEPLATFORMOK.HU: *Célkeresztben a TikTok: Bizottsági vizsgálatok*. 2024. április 30. <https://onlineplatformok.hu/cikk/celkeresztben-a-tiktok-bizottsagi-vizsgalatok> (letöltés: 2024. 05. 30.)

⁷³⁵ *Fitness Check i. m.* 345.

kiszolgáltatott csoportok, így a kiskorúak és az érzékeny adatokkal bíró felhasználók, fogyasztók védelmére, hiszen a célzott reklámozást, a kiszolgáltatott helyzetet csak a teljes tilalom szüntetheti meg.

2.2. Szerződések szabályozása

2.2.1. A UCT-irányelv – a tisztességtelen szerződési feltételekről

Az információs aszimmetria ellen ható fogyasztóvédelmi eszközrendszer jelentős eleme a szerződési feltételek szabályozása. A szabványszerződésekben tisztességtelen feltételek is előfordulhatnak, ezek ellen védi a fogyasztókat a UCT-irányelv. Hatálya olyan szerződési feltételekre terjed ki, amelyeket előre elkészítettek, és amelyeknek a tartalmát a fogyasztóval egyedileg nem tárgyalták meg, ebből következően a fogyasztónak nem volt rá befolyása. Ezek az általános szerződési feltételek. Abban az esetben beszélhetünk tisztességtelen szerződési feltételről, ha az ellentétes a jóhiszeműség követelményével, azaz a felek (az eladó vagy szolgáltató és a fogyasztó) szerződésből eredő jogaiban és kötelezettségeiben jelentős egyenlőtlenséget idéz elő a fogyasztó kárára.⁷³⁶ A UCT-irányelv melléklete tartalmazza a tisztességtelen feltételek jelzésszerű, de nem teljes felsorolását, ezt nevezik a szerződési feltételek feketelistájának is. Ezekkel az uniós jogalkotó iránymutatást nyújt a tagállami jogalkotók számára. A 2024 őszén közzétett Fitness Check tanulmány hiányossággént állapította meg, hogy a UCT-irányelvben szereplő szerződési feltételek feketelistája nem tartalmaz a digitális piacokra vagy a platformokra vonatkozó elemeket,⁷³⁷ másrészt a közelmúlt platformjogszabályai és a kapcsolódó ügyek is erőteljesen utalnak erre a hiányosságra, és megkívánják az irányelv harmonizálását a kapcsolódó jogszabályokkal.

A GDPR és a UCT-irányelv összefüggését példázza a Facebook kontra Bundeskartellamt ügy.⁷³⁸ A lehetséges jogalapok vizsgálata alapján azt láttuk (V. fejezet), hogy a Facebooknak egyetlen jogszerű jogalapja maradt: az érintett hozzájárulása, ezért az általános szerződési feltételekbe foglalta bele adatkezelési gyakorlatát, vagyis hogy nemcsak a közösségi hálózati szolgáltatásból származó személyes adatokat gyűjtötte, hanem más szolgáltatásokból, harmadik felek weboldalairól és alkalmazásaiból, cookie-kból stb. származó adatokat is, és ezeket, összekapcsolva a felhasználói fiókkal, felhasználta a célzott hirdetésekhez. Ez fölveti az érintett hozzájárulása érvényességének kérdéskörét, és fölveti a GDPR szerinti célhoz

⁷³⁶ UCT-irányelv 3. cikk

⁷³⁷ *Fitness Check* i. m. 346.

⁷³⁸ C-252/21. sz. ügy – Meta Platforms/Bundeskartellamt

kötöttség elvének és az adattakarékosság elvének kérdéseit is. E két elv különösen fontos az online szolgáltatásokra vonatkozó szerződések esetében, amelyek jellemzően szabványszerződések, ezért vonatkozik rájuk a UCT-irányelv (ill. annak tagországi harmonizációja). Ennek kapcsán fennáll annak akut kockázata, hogy az adatkezelők e szerződésekbe feltételként foglalják bele az adatkezelési gyakorlatukat azzal a céllal, hogy maximalizálják az adatok gyűjtését, kezelését anélkül, hogy e célokat megfelelően meghatároznák, vagy hogy figyelembe vennék az adattakarékossági kötelezettségeket.⁷³⁹ A Facebook is az általános szerződési feltételekbe foglalt adatkezelési gyakorlatával igyekezett kibújni a GDPR említett elvei alól.

2.2.2. A DCS-irányelv – a személyes adatok mint ellenérték

Az online tér bővülése és a weboldalakon keresztül, távollévők között kötött szerződések növekvő volumene azt kívánta, hogy a fogyasztóvédelmi szabályok az ún. ingyenes szolgáltatásokat igénybe vevőkre is kiterjedjenek. Ezzel összefüggésben a Bizottság az ingyenes digitális szolgáltatásokra vonatkozóan is szorgalmazta a fogyasztóvédelem kiterjesztését, ideértve a felhőalapú tárolást, a közösségi médiát és az e-mail-fiókokat. Érvelésében kifejtette, hogy ezek nem egyszerűen ingyenes szolgáltatások, mert a fogyasztók fizetnek értük, de nem pénzzel, hanem a személyes adataikkal, ezért ezeknek a fogyasztóknak ugyanazokkal a jogokkal kell rendelkezniük, mint azoknak, akik pénzzel fizetnek,⁷⁴⁰ vagyis biztosítani kell ugyanazokat a jogokat, amelyek a visszterhes szerződésekhez is kapcsolódnak.

Ezt az elvárást realizálta a DCS-irányelv, mely minden olyan szerződésre vonatkozik, amely alapján a kereskedő a fogyasztónak digitális tartalmat szolgáltat vagy digitális szolgáltatást nyújt; ezek körébe tartoznak például a digitális játékok, számítógépes programok, tárhelyszolgáltatások, közösségi média stb. (de nem tartoznak ide az internet-hozzáférési szolgáltatások),⁷⁴¹ valamint a kizárólag digitálistartalom-hordozóként használatos fizikai adathordozók is, például a memóriakártya.⁷⁴² Tárgyi hatályát tekintve nemcsak akkor kell alkalmazni, ha a fogyasztó a szolgáltatásért vételárat fizet, hanem akkor is, ha a kereskedő rendelkezésére bocsát személyes adatokat, ill. erre kötelezettséget vállal.⁷⁴³ A DCS-irányelv ezzel végeredményben elismerte a személyes adatok ellenszolgáltatásként használatának jogszerűségét, elismerte a felhasználó fogyasztó minőségét, és azon fogyasztók védelmére is

⁷³⁹ EDPB: 2/2019. 16. pont

⁷⁴⁰ COM(2018) 183 final. 2. pont

⁷⁴¹ DCS-irányelv (18)–(19) preambulumbekzdés

⁷⁴² DCS-irányelv (20) preambulumbekzdés és 3. cikk (3) bekezdés

⁷⁴³ DCS-irányelv 3. cikk (1) bekezdés

kiterjesztette a szabályozást, akik a weboldalon keresztül kötnek pénzbeli ellentételezés nélküli szerződést. Értelemszerűen a személyes adatok ellenszolgáltatásként használata a fogyasztói oldalon is megjelenik a CR-irányelvben.⁷⁴⁴ A DCS-irányelv elfogadása előtt az európai adatvédelmi biztos problémaként értékelte az adatok ellentételezésként történő felhasználását, ezzel együtt az adatok vonatkozásában e kifejezés használatát (ezért az irányelvben az „adatokat ad át,” ill. a „rendelkezésére bocsát” szerkezetek szerepelnek⁷⁴⁵), mivel a személyes adatok védelméhez való jog az alapvető jogok közé tartozik, tehát nem szűkíthető le pusztán a fogyasztói érdekekre, ebből következőn a személyes adatok nem tekinthetők csupán árunak.⁷⁴⁶

Az adatvédelmi biztos a GDPR-ral való összhang fontosságára is felhívta a figyelmet.⁷⁴⁷ A szerződésre vonatkozó követelményeket a személyes adatok átadására és kezelésére vonatkozó követelményekkel is össze kell hangolni, tekintve, hogy ez utóbbi egy másik jogterülethez, az adatvédelmi joghoz tartozik. A DCS-irányelv hatálya alá tartozó szerződések keretében végzett személyesadat-kezelés csak abban az esetben jogszerű, ha annak jogalapja megfelel a GDPR rendelkezéseinek.⁷⁴⁸ Ez a pont hordozza a feszültséget: az adatkezeléshez jogalap szükséges, az adat azonban nem válhat a szerződésben ellenszolgáltatássá. A digitális szolgáltatásra irányuló szerződések vonatkozásában jogalként a szerződés teljesítéséhez szükségesség nem jöhet szóba, mert az csak akkor alkalmazható, ha nélküle a szerződés nem lenne teljesíthető; a jogos érdekre hivatkozás érdekmérlegelési tesztet kíván, amely rámutat arra, hogy az érintett jogait nem írja felül a szolgáltató üzleti modelljéből következő adatkezelés (profilalkotás, adattovábbítás stb.);⁷⁴⁹ tehát a hozzájárulás tudja biztosítani az érintett fogyasztó rendelkezési jogát a személyes adatai felett, és ez alapján tudja a szolgáltató jogszerűen kezelni, használni ezeket az adatokat. Mindez a fogyasztó szempontjából, figyelembe véve azt, hogy hozzájárulását bármikor visszavonhatja – amely nem érinti a visszavonás előtti adatkezelés jogszerűségét⁷⁵⁰ –, monopolhelyzetet teremt, de ugyanakkor egyfajta tűrési kötelezettséget is eredményez,⁷⁵¹ kvázi olyan kiszolgáltatott helyzetet, mint amikor a Facebook az általános szerződési feltételekhez kötötte a regisztrációt, amely egyúttal a személyes adatok gyűjtésére stb. is módot adott. A különbséget abban kell látni, hogy a DCS-irányelv választási lehetőséget

⁷⁴⁴ CR-irányelv 3. cikk (1a) bekezdés

⁷⁴⁵ DCS-irányelv (24) preambulumbekzdés és 3. cikk (1) bekezdés

⁷⁴⁶ European Data Protection Supervisor: Opinion 4/2017. 3.

⁷⁴⁷ Opinion 4/2017. 21.

⁷⁴⁸ DCS-irányelv (38) preambulumbekzdés

⁷⁴⁹ GDPR 6. cikk

⁷⁵⁰ GDPR 7. cikk (3) bekezdés

⁷⁵¹ KOZMA Gábor Levente: *Quid pro quo: a személyes adat mint ellenszolgáltatás*. Versenytükör 2023. különszám. 80.

biztosít „a fizetendő pénzösszeg vagy digitális ellenérték”⁷⁵² vagylagos megnevezésével, amivel egyúttal legitimálja a hozzájárulás jogalapként használatát, az önkéntesség követelményének sérelme nélkül.⁷⁵³ Bár az önkéntességet még így is megkérdőjelezi az, hogy a pénzzel fizetés gazdasági kényszer, tehát nem valódi alternatíva; hosszabb távon elképzelhető, hogy a „megengedőbb értelmezés felé” fog elmozdulni az adatvédelmi gyakorlat.⁷⁵⁴ A szerződéseknek tartalmazniuk kell azokat a követelményeket, amelyek a digitális tartalom vagy a digitális szolgáltatás szerződészerű teljesítésére, a hibás teljesítésre és a jogorvoslati lehetőségekre vonatkoznak⁷⁵⁵ – hiszen éppen e célok motiválták az EU-t a jogszabályalkotás során –, kérdéses azonban, hogy a jelenlegi szabályok biztosítják-e a szükséges fogyasztóvédelmi garanciákat.⁷⁵⁶ Az adat mint ellenszolgáltatás típusú szerződés fogalmának definiálása által egyértelműen lehatárolhatók lennének a szerződő felek kötelezettségei.⁷⁵⁷

A DCS-irányelv elősegítette a személyes adatoknak az adatgazdaságba való becsatornázását,⁷⁵⁸ s előkészítette az utat, ami a Data Act megalkotásához vezetett. A DCS-irányelv és a Data Act annak a folyamatnak a része, amely a személyes adatok erőteljes védelmezése mellett ezen adatok gazdaságban betöltendő szerepét is előtérbe helyezi, illeszkedve a GDPR szelleméhez az adatok szabad áramlásának elősegítése tekintetében. Hatása révén tovább erősítette azoknak a piaci szereplőknek a gazdasági helyzetét, amelyeknek üzleti modellje az adatgyűjtésen alapul, valamint további ösztönzést adott nekik a már bevett – de nem mindig tisztességes – személyesadat-gyűjtési és -kezelési gyakorlatuk folytatásához.

2.2.3. A CR-irányelv – tájékoztatási kötelezettség és átláthatóság a távollévők között kötött szerződésekben

A CR-irányelv jelentőségét megalkotása idején, 2011-ben az adta, hogy az üzlethelyiségen kívül kötött szerződésekre vonatkozóan⁷⁵⁹ és a távollévők között kötött

⁷⁵² DCS-irányelv 2. cikk 7. pont

⁷⁵³ DUDÁS Gábor – ZAVODNYIK József: *A személyes adat mint ellenszolgáltatás a digitális szolgáltatások nyújtására irányuló szerződésekben*. 112–113. In: BODZÁSI Balázs (szerk.): *Gazdasági jogi és adójogi tanulmányok 2020*. Budapesti Corvinus Egyetem, 2020.

⁷⁵⁴ DUDÁS–ZAVODNYIK i. m. 114.

⁷⁵⁵ DCS-irányelv (11) preambulumbekkezdés

⁷⁵⁶ Rui Filipe Gordete ALMEIDA: *Os dados pessoais como contraprestação nos contratos de consumo — a necessidade para a execução do contrato como fundamento de licitude do tratamento* Personal data as counter-performance in consumer contracts — the necessity for the performance of a contract as a basis to ensure a lawful personal data processing. RED 2023/2. 14. DOI 10.24840/2182-9845_2023-0002_0002 (letöltés: 2025. 12. 30.)

⁷⁵⁷ ALMEIDA i. m. 31.

⁷⁵⁸ DARÁZS Lénárd: *Digitális fogyasztóvédelem európai perspektívában*. In: Salus vocalis. Csegöldi indulás – Győri érkezés. 89. DOI: 10.59199/salusvocalis.2023.10 (letöltés: 2024. 02. 12.)

⁷⁵⁹ Korábban: a fogyasztók védelméről szóló, 1985. december 20-i 85/577/EGK tanácsi irányelv

szerződésekre vonatkozóan⁷⁶⁰ megerősítette a fogyasztói jogokat, ill. a korábbi két irányelvet egyetlen irányelv váltotta fel.⁷⁶¹ Célja szerint a belső piac megfelelő működéséhez kíván hozzájárulni azáltal, hogy közelíti a fogyasztók és kereskedők között kötött szerződésekre vonatkozó tagállami rendelkezéseket,⁷⁶² valamint – az omnibusz irányelv által beillesztett rendelkezéseknek köszönhetően – ösztönzi az online vásárlást.

A CR-irányelv középponti elvárása a tájékoztatási kötelezettség, amely a más módon kötött szerződésekhez képest többletkötelezettségeket ír elő a távollévők között kötött és az üzlethelyiségen kívül kötött szerződések tekintetében. A tájékoztatási kötelezettségnek ki kell terjednie a kereskedőt azonosító adatokra, a termék főbb jellemzőire és a vonatkozó feltételekre, valamint arra, hogy az ár automatizált döntéshozatal alapján személyre szabott-e,⁷⁶³ amely azonban csak olyan szerződések esetén releváns, amelyek lehetővé teszik az automatizált döntéshozatalt és profilalkotást.⁷⁶⁴ A kereskedők – a GDPR vonatkozó rendelkezései alapján – gyűjtik az egyes fogyasztók személyes adatait, azokat algoritmusokkal, automatizált elemzéssel feldolgozzák, ez alapján készül a profil. A kötelező tájékoztatás a személyre szabás tényére vonatkozó információra korlátozódik.⁷⁶⁵ Ez a tájékoztatási követelmény kiegészíti a GDPR-t azzal, hogy adott értékesítési helyen is megköveteli az átláthatóságot.⁷⁶⁶

Az online piacon kötött szerződésekre vonatkozóan egyedi kiegészítő tájékoztatási követelményeket illesztett a CR-irányelvbe az omnibusz irányelv. E követelmények értelmében a kereskedőnek az átláthatóságot biztosító minden szükséges információval el kell látnia az online platformokon vásárló fogyasztókat még a szerződés megkötése előtt, hogy a megalapozott döntések meghozatalában támogassa őket. E cél érdekében – mivel az online piacon a fogyasztók nemcsak a kereskedőkkel, hanem harmadik felekkel is kapcsolatba kerülhetnek, és szerződést köthetnek⁷⁶⁷ – kötelező tájékoztatni a fogyasztókat világos és érthető nyelven a keresés nyomán megjelenő ajánlatok rangsorolását meghatározó fő paramétereiről. A rangsorolás relatív kiemeléssel történik, a fő paraméter a rangsorolással összefüggésben

⁷⁶⁰ Korábban: a fogyasztók védelméről szóló, 1997. május 20-i 97/7/EK európai parlamenti és tanácsi irányelv

⁷⁶¹ CR-irányelv (1) preambulumbekzdés

⁷⁶² CR-irányelv 1. cikk

⁷⁶³ CR-irányelv 6. cikk

⁷⁶⁴ 2021/C 525/01. A Bizottság közleménye a fogyasztók jogairól szóló 2011/83/EU európai parlamenti és tanácsi irányelv értelmezésére és alkalmazására vonatkozó iránymutatásról. 3.3.1. pont

⁷⁶⁵ 2021/C 525/01. 3.3.1. pont

⁷⁶⁶ COM(2024) 258 final. A Bizottság jelentése az Európai Parlamentnek és a Tanácsnak a 93/13/EGK tanácsi irányelvnek, valamint a 98/6/EK, a 2005/29/EK és a 2011/83/EU európai parlamenti és tanácsi irányelvnek az uniós fogyasztóvédelmi szabályok hatékonyabb végrehajtása és korszerűsítése tekintetében történő módosításáról szóló, 2019. november 27-i (EU) 2019/2161 európai parlamenti és tanácsi irányelv végrehajtásáról. Brüsszel, 2024. 06. 18. 36.

⁷⁶⁷ CR-irányelv 3. cikk 17. pont

használt bármely kritérium, algoritmusokba épített különös jel vagy más mechanizmus lehet.⁷⁶⁸ Tájékoztatni kell arról is, hogy az említett harmadik fél kereskedőnek minősül-e, vagy nem (az online piac szolgáltatója felé tett nyilatkozata alapján). Utóbbi esetben gyakorlatilag egy másik fogyasztóról van szó, ebből következően az uniós fogyasztóvédelmi jogszabályokból eredő fogyasztói jogok nem alkalmazhatók a szerződésre, s erről is tájékoztatni kell a fogyasztót. Végül arról, hogy ki a felelős a szerződés teljesítéséért: a harmadik félnek minősülő kereskedő vagy maga az online piactér, esetleg megoszlik a felelősség.⁷⁶⁹ Az utóbbi két elem esetében a transzparencia kulcsfontosságú, mert biztosítja, hogy a fogyasztók tisztában legyenek jogaikkal vagy azok hiányával. Összefüggésben áll ez a DSA által az online platformokra rótt, hirdetésekkel kapcsolatos tájékoztatási kötelezettségekkel.⁷⁷⁰

A CR-irányelv a kereskedők és fogyasztók között kötött bármely szerződésre alkalmazandó, amikor a fogyasztó kifizeti vagy vállalja, hogy kifizeti az árat; és hatálya kiterjed azon szerződésekre is, amelyek keretében a kereskedő digitális szolgáltatást vagy tartalmat nyújt, vagy vállalja annak nyújtását, a fogyasztó pedig személyes adatok szolgáltatását vállalja. De nem terjed ki a hatálya azon szerződésekre, amelyekben a személyes adatok kezelésére kizárólag a szerződés teljesítése és a jogi következményeknek való megfelelés céljából kerül sor, és a kereskedő semmilyen más célból nem kezeli azokat.⁷⁷¹ Ebből az is következik, hogy a kereskedő, aki egyúttal adatkezelő is, kétféle GDPR-jogalap alapján kezeli a személyes adatokat: egyrészt a szerződés teljesítéséhez szükségesség jogalapjára hivatkozva, valamint a szerződés teljesítéséhez nem szükséges adatkezelési műveletek esetében például a hozzájárulásra hivatkozva.⁷⁷²

A CR-irányelv jelentőségét – a tájékoztatási kötelezettségek előírásán túl – az adja, hogy elősegíti a személyes adatok beépülését az adatgazdaságba, megalapozza a GDPR alapján az adatok szabad áramlásának realitását, növelve ezek által az EU digitális lehetőségeit.

2.3. A UCP-irányelv – a tisztességtelen kereskedelmi gyakorlatok tilalma

A tisztességtelen kereskedelmi gyakorlat olyan tevékenység vagy mulasztás – a kereskedelmi ügylet lebonyolítását megelőzően, a lebonyolítás során vagy azt követően –, amely közvetlen kapcsolatban áll valamely terméknek a kereskedő által a fogyasztó részére

⁷⁶⁸ Omnibusz irányelv (22) preambulumbekzdés

⁷⁶⁹ CR-irányelv 6a. cikk

⁷⁷⁰ DSA 26. cikk

⁷⁷¹ CR-irányelv 3. cikk (1)–(1a) bekezdés, beiktatta az omnibusz irányelv

⁷⁷² GDPR 6. cikk (1) bekezdés b) és a) pont

történő eladásösztönzésével, értékesítésével vagy szolgáltatásával.⁷⁷³ Adott kereskedelmi gyakorlat akkor tisztességtelen, ha ellentétes a szakmai gondosság követelményével, és ha jelentősen torzíthatja az átlagfogyasztó vásárlási magatartását.⁷⁷⁴ Két kategóriája van: a megtévesztő (amely akár tevékenységgel, tehát aktívan; akár mulasztással, tehát passzívan valósulhat meg) és az agresszív kereskedelmi gyakorlat.⁷⁷⁵ A platform–kereskedő–fogyasztó háromszereplős modelljének erősödése megkövetelte az online piac fogalmának beillesztését és meghatározását a UCP-irányelvben: olyan szolgáltatás, amely a kereskedő által vagy az ő nevében működtetett szoftvert (weboldalt vagy alkalmazást) alkalmaz, és amely lehetővé teszi a fogyasztók számára, hogy távollevők közötti szerződést kötssenek más kereskedőkkel vagy fogyasztókkal.⁷⁷⁶

Az online piacok lendülete korábban nem ismert tisztességtelen kereskedelmi gyakorlatokat termelt ki, melyek közül néhány a UCP-irányelv feketelista-mellékletében is helyet kapott: a fogyasztói értékelések, a keresési eredményekben a fizetett reklámok és rangsorolás, valamint a rendezvényre szóló jegyek viszonteladása tekintetében, ill. a szoftverfrissítéssel kapcsolatos állítások.⁷⁷⁷ E melléklet által védi a gyermekeket is – bár az őket célzó reklámokat nem tiltja – a vásárlásra való közvetlen felszólításoktól, azaz agresszív kereskedelmi gyakorlatnak minősíti a reklámban a gyermekek közvetlen felszólítását a termék megvásárlására, vagy akár arra, hogy meggyőzzék szüleiket vagy más felnőttet, hogy vásárolja meg számukra a reklámozott terméket.⁷⁷⁸

Mindezek mellett feltűnik azonban, hogy a UCP-irányelv egyáltalán nem utal az adatok, a személyes adatok jelentőségére, noha ezek alapvető fontosságúak sok kereskedő üzleti modellje és a fogyasztók szempontjából egyaránt. Az adatokra való hivatkozások hiánya miatt a UCP-irányelv elavultnak tűnik, modernizálása szükséges. Az adatokra való hivatkozás hiányának következménye az, hogy a UCP-irányelv feketelistájában nincsenek konkrétan nevesítve a tisztességtelen kereskedelmi gyakorlatok között a személyes adatokkal összefüggésbe hozható tiltott gyakorlatok, köztük a sötét megoldások (dark patterns).⁷⁷⁹ A Bizottság iránymutatása szerint a UCP-irányelv elvi alapú rendelkezései és tilalmai alkalmasak

⁷⁷³ UCP-irányelv 2. cikk d) pont és 3. cikk (1) bekezdés

⁷⁷⁴ UCP-irányelv 5. cikk (2) bekezdés

⁷⁷⁵ UCP-irányelv 5. cikk (4) bekezdés

⁷⁷⁶ UCP-irányelv 2. cikk n) pont, beiktatta az omnibusz irányelv

⁷⁷⁷ UCP-irányelv I. melléklet: az omnibusz irányelv által beiktatott 11a. pont és 23a.–23c. pontok, valamint az Európai Parlament és a Tanács 2024/825 irányelve által beiktatott 23d.–23e. pontok

⁷⁷⁸ UCP-irányelv (18) preambulumbekkezdés és 1. melléklet 28. pont

⁷⁷⁹ A fogalmat 2010-ben használta először egy a felhasználói élmény tervezésével foglalkozó UY designer. A dark patterns jelentését Magyarországon a sötét minták, sötét megoldások kifejezéssel adják vissza, a DSA az utóbbit használja.

azon tisztességtelen kereskedelmi gyakorlatok kezelésére is, amelyek a sötét megoldások körébe tartoznak.⁷⁸⁰ Ugyanakkor ezek alkalmazhatóságát nehezíti az, hogy a UCP-irányelvet a kereskedők és a fogyasztók közötti közvetlen tranzakciókra tervezték, és nem a közvetítő jellegű platformokra,⁷⁸¹ következésképpen az aszimmetriát sem tudják hatékonyan kezelni.

Véleményem szerint a személyes adatokkal kapcsolatban felmerülő tiltott gyakorlatok rögzítése feketelistán két jelentős előnyt is hordozna. Egyik előnye az, hogy a lista egyértelmű állításokat tartalmaz, ami különösen azért fontos, mert a tisztességes és a tisztességtelen fogalmak jelentésének elhatárolása nem egyszerű feladat, s ehhez a UCP-irányelv a cikkeiben alig ad kapaszkodót. Másik előnye az, hogy ha adott kereskedői magatartás a UCP-irányelv feketelistájában szerepel, akkor az a jogszabály erejénél fogva, ex lege tisztességtelen kereskedelmi gyakorlatnak minősül, és elegendő azt bizonyítani, hogy a kereskedő az adott magatartást valóban megvalósította. Ebből következően könnyebb és kevésbé időigényes a bizonyítás, mintha nem szerepel a feketelistában; akkor ugyanis előbb azt kell egyedileg vizsgálni, hogy az adott kereskedelmi gyakorlat megfelel-e a megtévesztő vagy az agresszív kereskedelmi gyakorlat ismérveinek. Ezzel kapcsolatban fontos hangsúlyozni, hogy ezek a javaslatok is kifejezetten a UCP-irányelv hatálya alá tartozó magatartásokat illetően relevánsak, mintegy kiegészítve a DSA-t, amely az online interfészek megtévesztő, torzító tervezésére vonatkozó tilalmakat, legalábbis az online platformok vonatkozásában, már tartalmazza.

A UCP-irányelvben – véleményem szerint – mindenképpen elő kellene írni a következőt: minden olyan szolgáltató, amely személyes adatokon alapuló személyre szabást alkalmaz, köteles legyen nem személyre szabott alternatívát is kínálni a fogyasztók számára. Ez hasonló javaslat, mint ami a DMA-ben már létezik, de ott csak a kapuőrökre vonatkozik; ill. a DSA alapján is tilos a profilalapú reklám, de csak a kiskorúakra és a különleges adatokkal rendelkezőkre vonatkozóan.⁷⁸² A javasolt rendelkezést egyrészt a cikkek közé illeszteném, kiegészítve ezzel a tisztességtelenség fogalmát; másrészt a feketelistában konkrét tiltásként fogalmaznám meg az egyenértékű alternatíva hiányát.

A UCP-irányelv rendelkezéseit Magyarországon a fogyasztókkal szembeni tisztességtelen kereskedelmi gyakorlat tilalmáról szóló Fttv. implementálta, ez alapján az eljáró hatóság, néhány kivételtől eltekintve, a fogyasztóvédelmi hatóság. Az egyik kivétel értelmében,

⁷⁸⁰ 2021/C 526/01. 4.2.7. fejezet

⁷⁸¹ Catalina GOANTA – Giovanni DE GREGORIO – Jerry SPANAKIS: *Consumer Protection and Digital Vulnerability: Common and Diverging Paths*. In *The New Shapes of Digital Vulnerability in European Private Law*. 2024. 44. <https://www.nomos-elibrary.de/10.5771/9783748940913-31/consumer-protection-and-digital-vulnerability-common-and-diverging-paths?page=3> (letöltés: 2025. 02. 02.)

⁷⁸² DMA 5. cikk (2) bekezdés; DSA 26. cikk (3) bekezdés és 28. cikk

ha a tisztességtelen kereskedelmi gyakorlat alkalmas a gazdasági verseny érdemi befolyásolására, akkor a GVH⁷⁸³ végez vizsgálatot. A GVH versenyfelügyeleti eljárás keretében állapította meg, hogy a Booking.com a honlapján és mobilalkalmazásában 2015. június 1-jétől a szálláskeresési és -foglalási folyamat lépéseinél a fogyasztót sürgető tájékoztatásokat tett közzé (pl. nagyon keresett; csak egy szoba maradt), amelyeket különböző színekkel, betűmérettel stb. is kiemelt. A sürgetésként és pszichológiai nyomásgyakorlásként azonosított sötét megoldások befolyásolhatták a fogyasztók tájékozott döntési folyamatát, és olyan üzleti döntés meghozatalára készíthették őket, amelyet egyébként nem hoztak volna meg, ezért a GVH agresszív kereskedelmi gyakorlat folytatása miatt állapított meg jogsértést az Fttv. 8. § (1) bekezdése alapján.⁷⁸⁴ Többek között sötét megoldások – sürgetés, pszichológiai nyomásgyakorlás és kényszerített játékok alkalmazása – miatt folytat vizsgálatot a Temuval szemben a GVH versenyfelügyeleti eljárás keretében, a fogyasztókkal szembeni tisztességtelen kereskedelmi gyakorlat tilalmának feltételezett megsértése miatt. Mivel határokon átnyúló ügyről van szó, a Fogyasztóvédelmi Együttműködési Hálózat (Consumer Protection Cooperation Network, CPC) összehangolt fellépés keretében felszólította a kínai piacteret, hogy az európai fogyasztóvédelmi szabályokkal hozza összhangba a kereskedelmi gyakorlatait; továbbá a Bizottság a DSA megsértése miatt indított eljárást.⁷⁸⁵ A Booking-ügyben jelentős érv volt az, hogy a sötét megoldások alkalmazása tekintetében nemcsak a szobafoglalás tekinthető üzleti döntésnek, hanem a keresési folyamat megkezdésétől egészen a foglalás véglegesítéséig fennállt, összhangban azzal, hogy a tisztességtelen kereskedelmi gyakorlat a kereskedelmi ügylet lebonyolítását megelőzően, a lebonyolítás során és azt követően is releváns.⁷⁸⁶

A sötét megoldások nemcsak a UCP-irányelv, ill. az implementált tagállami jogszabályok megsértését jelenthetik, hanem több jogterület, több jogszabály is érintett lehet. Különösen így van ez az online platformok esetében, amelyek adatokat gyűjtenek, kezelnek, valamint közvetítő felületet biztosítanak a felhasználók/fogyasztók–árúk–információk között.

2.4. Sötét megoldások az online platformok gyakorlatában

Az online platformok üzleti tevékenységének alapja az adatgyűjtő és -kezelő tevékenység, ezért igyekeznek minél több személyes adatot megszerezni, és minél összetettebben, profilalkotással, algoritmusokkal kezelni azokat. A másik oldalon a jogalkotók

⁷⁸³ Fttv. 10. § (1) és (3) bekezdés

⁷⁸⁴ VJ/28-61/2022.

⁷⁸⁵ GVH: *Összehangolt európai fellépés a Temu-val szemben*. Sajtóközlemény, 2024. 11. 08. [Összehangolt európai fellépés a Temu-val szemben - GVH](#) (letöltés: 2024. 12. 10.)

⁷⁸⁶ Fttv. 1. § (1) bekezdés (UCP-irányelv 3. cikk (1) bekezdés)

a GDPR bevezetése óta azonban egyre célzottabb jogszabályokat alkotnak az említett folyamat megállítására, de legalább kontrollálására, ill. az adatgazdaság szabályok közé szorított támogatására. E szakadék feloldására a platformok az információs aszimmetriából eredő hátrányokat kihasználva próbálják magukat az érintetteket, a felhasználókat és a fogyasztókat manipulálni, észrevétlenül rábírní arra, hogy adataikat önként adják át, s ehhez a sötét megoldásokat használják. A sötét megoldások alkalmazásának célja nemcsak az adatok megszerzésére és kezelésére irányul, hanem ezzel szoros kapcsolatban a felhasználó figyelmének felkeltésére és manipulálására abból a célból, hogy tényleges fogyasztóvá váljon.

A sötét megoldások definiálása nem egyszerű feladat, főleg a technológiai háttér dinamizmusa miatt, valamint e megoldások sokszínűsége miatt. Petrányi Dóra és szerzőtársai tizenegy szakirodalmi műben és jogszabályban található meghatározásból szűrték le a főbb jellemzőket, ez alapján a sötét megoldásokat azonosító elemek a következők: A felhasználói felületen jelennek meg, amihez a platformok olyan interfészeket használnak, amelyekkel előre megtervezhetik azt az útvonalat, amelyet a felhasználóknak végig kell járniuk, ezáltal képesek a céljaiknak megfelelő manipulatív gyakorlatokat beilleszteni (9 előfordulás). Megtévesztő és leplezett jellegűek, vagyis a felhasználók nincsenek tisztában a felhasználói felület befolyásoló, félrevezető hatásával (6 előfordulás). 3-4-szer az is előfordul, hogy a felhasználó döntéseit befolyásolják, számára anyagi (észrevétlen előfizetés) vagy nem anyagi kárt okoznak (adatai feletti rendelkezés elvesztése); s mindig szándékos tevékenység a kereskedő részéről.⁷⁸⁷

A sötét megoldások a tipikus jegyeik, a felhasználóra gyakorolt hatásuk stb. mentén kategorizálhatók; többféle szempontú osztályozási lehetőségeiket számos tanulmány tárta fel.⁷⁸⁸ Szabályozásuk egyelőre – hasonlóan a fogyasztóvédelmi szabályozás széttagoltságához – több jogág, jogterület jogszabályai által lehetséges, ezért adott sötét megoldásnál mindig vizsgálandó az, hogy melyik jogszabály megsértéséről van szó. Az érintett jogágak, jogterületek és jogszabályok, valamint a tipikus, gyakori sötét megoldások kapcsolatát mutatja a 7. táblázat, alapvetően azokra a megoldásokra koncentrálva, amelyek a személyes adatokkal kapcsolatba

⁷⁸⁷ PETRÁNYI Dóra – DOMOKOS Márton – HORVÁTH Anna Zsófia – HUSZÁR Daniella: *Az online platformokon alkalmazott sötét megoldások*. 2023. július 4. 8–9. <https://onlineplatformok.hu/files/21982413-9a9f-4e6f-b6b5-2530bda6d7ed.pdf> (letöltés: 2024. 01. 01.)

⁷⁸⁸ Arunesh MATHUR – Jonathan MAYER – Mihir KSHIRSAGAR: *What Makes a Dark Pattern... Dark? Design Attributes, Normative Considerations, and Measurement Methods*. Proceedings of the 2021 CHI Conference on Human Factors in Computing Systems, 2021. 1–18. <https://doi.org/10.1145/3411764.3445610> (letöltés: 2023. 12. 21.); M. R. LEISER: *Illuminating Manipulative Design: from „Dark Patterns” to Information Asymmetry and the Repression of Free Choice under the Unfair Commercial Practices Directive*. 2022. 1–30. <http://dx.doi.org/10.2139/ssrn.4418586> (letöltés: 2024. 08. 04.); PETRÁNYI–DOMOKOS–HORVÁTH–HUSZÁR i. m. 1–56.

hozhatók. A teljesség érdekében nemcsak azokat a jogszabályokat tartalmazza a táblázat, amelyeket e fejezetben áttekintettem, hanem a GDPR-t és a versenyjognál vizsgáltakat is.

7. táblázat: Jellemző sötét megoldások és a vonatkozó uniós jogszabályok

ADATVÉDELEM	
1.) GDPR	
Jogszabályhely	Sötét megoldások
GDPR 5. cikk (1) bekezdés a) pont = <i>jogszerűség, tisztességes eljárás, átláthatóság</i>	• adatvédelmi útvesztő • felkavaró sötét megoldások
GDPR 5. cikk (1) bekezdés b)–c) pont = <i>célhoz kötöttség, adattakarékosság</i>	• többletselekvések • ismétlődő kérések • újra felugró ablakok
GDPR 4. cikk 11. pont és 6–7. cikk = <i>hozzájárulás</i>	• előválasztás • vizuális kiemelések • előre kipipált jelölőnégyzet
GDPR 12–14. cikk = <i>tájékoztatáshoz való jog</i>	• sehová nem mutató linkek (linkzsákutca) • bonyolult/homályos nyelvezet • ellentmondó információk
GDPR 21. cikk = <i>tiltakozáshoz való jog</i>	• bonyolult/homályos nyelvezet • logikátlan elhelyezés
GDPR 25. cikk = <i>beépített és alapértelmezett adatvédelem</i>	• rejtett információk • kényszerregisztráció • előre bepipált jelölőnégyzetek • bonyolult/homályos nyelvezet
2.) ELEKTRONIKUS HÍRKÖZLÉSI ADATVÉDELMI IRÁNYELV (cookie-k) (2002/58/EK)	
Jogszabályhely	Sötét megoldások
Elektronikus hírközlési adatvédelmi irányelv 5. cikk (3) bekezdés = <i>hozzájárulás hirdetési célú cookie-k elhelyezéséhez</i>	• vizuális kiemelések • kényszerített cselekvés (kötegetelt hozzájárulás → gomb: összes elfogadása)
Elektronikus hírközlési adatvédelmi irányelv 13. cikk = <i>nem kívánt tájékoztatás</i>	• spam • csótánymotel • álcázott hirdetések
FOGYASZTÓVÉDELEM	
1.) UCP-irányelv	
Jogszabályhely	Sötét megoldások
UCP-irányelv 5. cikk (2) bekezdés = <i>tisztességtelen kereskedelmi gyakorlatok tilalma</i>	• UCP-irányelv I. melléklet 1–23. pontjai (fogyasztó gazdasági magatartásának torzítása), pl. ingyenesség látszatának keltése
UCP-irányelv 8–9. cikk = <i>agresszív kereskedelmi gyakorlatok tilalma</i>	• pszichológiai nyomásgyakorlás • sürgetés

	• kényszerített játékok • rejtett feliratkozás, előfizetés • csótánymotel (nehéz lemondás) • UCP-irányelv I. melléklet 23a.–31. pontjai (fogyasztó választási szabadságának jelentős korlátozása), pl. tartós nyaggatás marketingüzenetekkel, gyermekek közvetlen felszólítása termékvásárlásra (szüleik nyaggatása), nyereménnyel csalogatás, online játékok függőséget okozó gyakorlatai
2.) CR-irányelv	
Jogszályhely	Sötét megoldások
CR-irányelv 6. cikk = <i>tájékoztató a távollevők között kötött szerződések esetében</i>	• rejtett költségek • halhatatlan fiók
CR-irányelv 8. cikk = <i>távollévők között kötött szerződések formai követelményei</i>	• rejtett előfizetés • kényszerű folytonosság
CR-irányelv 16e. cikk = <i>kiegészítő védelem az online interfészek tekintetében (távértékesítés útján kötött pénzügyi szolgáltatásokra vonatkozó szerződések)</i>	• választási lehetőség nem semleges módon biztosítása • ismételt felkérés (felugró ablak) • csótánymotel (pókhálómódszer)
3.) UCT-irányelv	
Jogszályhely	Sötét megoldások
UCT-irányelv 3. cikk = <i>ÁSZF – szerződési feltételei</i>	• a mellékletben (feketelista) felsoroltak
UCT-irányelv 5. cikk = <i>ÁSZF – világos és érthető feltételek</i>	• bonyolult nyelvezet • apró betűs részek • rejtett záradékok • kétértelműség
PLATFORMJOGSZABÁLYOK	
1.) DMA	
Jogszályhely	Sötét megoldások
DMA (63) preambulumbekzdés és DMA 13. cikk (6) bekezdés = <i>kijátszás tilalma (platformszolgáltatások minősége)</i>	• pókhálómódszer/csótánymotel (fiók megszüntetése, leiratkozás megnehezítése) • választási lehetőség nem semleges módon biztosítása • interfészkiakításhoz kapcsolódó sötét megoldások
2.) DSA	
Jogszályhely	Sötét megoldások

DSA 25. cikk (1) bekezdés és (3) bekezdés = <i>online interfész tervezése, kialakítása</i>	• vizuális kiemelések • ismételt felkérés (felugró ablak) • csótánymotel (pókhálómódszer)	bizottsági iránymutatás várható
3.) Data Act		
Jogszabályhely	Sötét megoldások	
Data Act 4. cikk (4) bekezdés és 6. cikk (2) bekezdés a) pont = <i>online interfész tervezése, kialakítása</i>	• választási lehetőség nem semleges módon biztosítása • interfészalkialakításhoz kapcsolódó sötét megoldások	

Forrás: saját szerkesztés PETRÁNYI–DOMOKOS–HORVÁTH–HUSZÁR i. m. 12–21.; EUROPEAN COMMISSION: *Behavioural study on unfair commercial practices in the digital environment: dark patterns and manipulative personalisation*. Final Report. 2022. 1–303. <https://data.europa.eu/doi/10.2838/859030> (letöltés: 2023. 06. 01.), valamint a hivatkozott jogszabályok alapján

A 7. táblázat alapján az látszik, hogy vannak olyan sötét megoldások, amelyek több jogszabály által is megközelíthetők. A csótánymotel alkalmazása gyakori sötét megoldás, azt jelenti, hogy a felhasználót fogva tartja a weblap vagy a platform, és megnehezíti vagy lehetetlenné teszi a leiratkozást a hírlevélről vagy a szolgáltatásról. Ha ez a sötét megoldás például annak kapcsán áll fenn, hogy a potenciális vásárló feliratkozott egy webáruház hírlevelére, de később a leiratkozási szándékát a weblap sötét megoldással akadályozza, akkor az a GDPR megsértését jelenti. Ha adott webáruházban a fogyasztó a kosárba helyez egy terméket, de azt csak az előző műveletnél hosszabb és nehezebb folyamattal tudja eltávolítani, akkor agresszív kereskedelmi gyakorlat valósul meg, és a UCP-irányelv hatálya alá tartozik. Ha azonban a felhasználó egy online platformon keresztül fiókot regisztrált, de ezt a fiókot nem tudja ugyanolyan egyszerűen lemondani, mint amikor regisztrált, akkor annak oka lehet az, hogy a közvetítő szolgáltatás úgy alakította ki az interfészeit, hogy az akadályozza a lemondást, és ez esetben a DSA hatálya alá fog tartozni. Úgy is fogalmazhatunk, hogy olyan sötét megoldások esetében kell a DSA-t alkalmazni, amelyek nem tartoznak a GDPR és a UCP-irányelv hatálya alá.⁷⁸⁹

A sötét megoldásokkal kapcsolatban nemcsak jogszabályi rendelkezések szükségesek, hanem gyakorlati segítséget nyújtó egyéb eszközök is. A GDPR alapelveiből (adattakarékosság, célhoz kötöttség stb.) levezethető a manipulatív gyakorlatok tilalma. Mivel ezek implicit módon korlátozzák a sötét megoldások használatát, fontos a szóba jöhető típusok bemutatása és értelmezése, ami – a közösségimédia-platformok gyakorlatára vonatkozóan – az EDPB iránymutatásában kapott helyet. Az iránymutatás e gyakorlatokkal összefüggésben a

⁷⁸⁹ DSA 25. cikk (2) bekezdés

beépített és alapértelmezett adatvédelem elveinek következetes alkalmazási lehetőségeire, valamint az adatvédelmi irányítópult bemutatására is felhívja a figyelmet.⁷⁹⁰

2.4.1. Sötét megoldások a platformjogszabályokban

A DMA – bár nem használja a sötét megoldás kifejezést – fogyasztóvédelmi célú rendelkezéseinek egyik szegmensét a sötét megoldások tilalmára vonatkozó szabályozás alkotja. A preambulumban a végfelhasználók (akik bármikor dönthetnek a kapuőr adatkezelési gyakorlatának elfogadásáról) hozzájárulásának visszavonását illetően előírja, hogy olyan egyszerűnek kell lennie, mint a megadása volt, ezért ehhez a kapuőrök számára megtiltja az online interfészek kialakítása során a végfelhasználókat megtévesztő, manipuláló, befolyásoló megoldások alkalmazását.⁷⁹¹ Ugyanez a cél érvényesül abban is, hogy a végfelhasználók szabadon választhatják meg, melyik alapvető platformszolgáltatást veszik igénybe, ezért egy alapvető platformszolgáltatással összefüggésben a fiók megszüntetése vagy a leiratkozás nem lehet bonyolultabb, mint annak létrehozása vagy a szolgáltatásra való előfizetés volt.⁷⁹² A felhasználói hozzájárulás visszavonása, a leiratkozás vagy a fiók megszüntetése tekintetében a DMA körülírja a kapuőr számára megtiltott sötét megoldást, amit vagy a csótánymotel, vagy a pókhálómódszer névvel illetnek a szakirodalomban,⁷⁹³ hiszen a fogyasztót fogva tartó és a kiszabadulását jelentősen nehezítő, esetleg lehetetlenné tévő módszerről van szó.

A DMA a kapuőrökre vonatkozó kötelezettségek kijátszását megakadályozó intézkedéseket is tartalmaz: nem ronthatják le az alapvető platformszolgáltatások minőségét abban az esetben sem, ha a végfelhasználók nem adták hozzájárulásukat a személyes adataik online hirdetési szolgáltatások nyújtása céljából való felhasználására, valamint ha éltek más jogaikkal,⁷⁹⁴ ami azt is jelenti, hogy e jogok gyakorlását nem nehezíthetik indokolatlan mértékben, tehát a kapuőrnek az interfészeit úgy kell kialakítania, hogy semleges módon biztosítson választási lehetőséget az említett felhasználók számára, ne ássa alá az autonómiájukat, döntéshozatalukat vagy szabad választásukat.⁷⁹⁵ E rendelkezés értéke az, hogy előzetesen szabályoz (ex ante), és hogy a műszaki megoldások szintjén interfészkialakítással szorgalmazza a sötét megoldások elleni fellépést. Ugyanakkor maga a kijátszási tilalom kifejezetten csak az 5–7. cikkekben foglaltakra vonatkozik, és nem az interfészkialakítással

⁷⁹⁰ EDPB: 03/2022. számú iránymutatás a közösségimédia-platformok interfészein előforduló megtévesztő tervezési megoldásokról: hogyan ismerjük fel és kerüljük el őket. 2.0. változat

⁷⁹¹ DMA (37) preambulumbekkezdés

⁷⁹² DMA (63) preambulumbekkezdés

⁷⁹³ PETRÁNYI–DOMOKOS–HORVÁTH–HUSZÁR *i. m.* 5., 16., 20.

⁷⁹⁴ DMA (36)–(37) preambulumbekkezdés és 13. cikk (6) bekezdés

⁷⁹⁵ DMA (70) preambulumbekkezdés és 13. cikk (6) bekezdés

összefüggő általános tilalomként került megfogalmazásra. A BEUC álláspontja szerint ez a rendelkezés nem elegendő a fogyasztók sötét megoldásokkal szembeni védelmére, ami fölveti azt is, hogy a sötét megoldások többsége továbbra is a UCP-irányelv hatálya alá tartozik.⁷⁹⁶

A UCP-irányelv – mely nem használja a sötét megoldás kifejezést – nemcsak a DMA hatálya alá nem tartozó sötét megoldásokkal kapcsolatban alkalmazható, hanem azokban az esetekben is, amelyekre a DSA nem vonatkozik, a DSA ugyanis csak az online platformokra vonatkozóan rendelkezik a sötét megoldásokkal összefüggésben.⁷⁹⁷ Ebből következően a többi online közvetítő szolgáltatóval kapcsolatban fölmerülő sötét megoldás szintén az üzleti vállalkozások és a fogyasztók viszonyában értelmezhető UCP-irányelv hatálya alá tartozik.

A DMA-tól szélesebb körben és a sötét megoldás kifejezést is használva – a saját szabályozási célja mentén tett definíciószerű állítások alapján – állapít meg tilalmakat a DSA. E definíciós elemek a sötét megoldások három jellemzőjét emelik ki: online interfészeken jelennek meg, jelentősen torzító vagy korlátozó hatásúak, és ezáltal a szolgáltatás igénybe vevőinek önálló és megalapozott döntéshozatali képességét befolyásolják.⁷⁹⁸ E jellemzők indokolják a sötét megoldások tilalmát az online platformot üzemeltető szolgáltatók számára: tilos a szolgáltatás igénybe vevőinek, a fogyasztóknak a megtevesztése vagy ösztönzése, valamint autonómiájuk, döntéshozataluk vagy választásuk torzítása vagy akadályozása – egy online interfész egészének vagy részének szerkezete, kialakítása vagy funkciói révén.⁷⁹⁹ A cél és a műszaki megoldás a DMA-ben is hasonlóan került megfogalmazásra, de a DSA néhány sötétmegoldás-típust is felsorol: a választási lehetőségek nem semleges módú bemutatása; ismételt felkérés választásra; lemondás, vásárlástörlés vagy platformról lejelentkezés indokolatlan megnehezítése stb.,⁸⁰⁰ elhatárolva egyúttal a sötét megoldásokat és a hirdetéseket egymástól, az utóbbiakhoz rendelt átláthatósági követelmények felsorolásával.⁸⁰¹

A konkrét rendelkezések szintjén a DSA egész cikket szán az online platformok kötelezettségeinek az interfész tervezése és kialakítása tekintetében: ezeket nem tervezhetik oly módon, hogy a fogyasztók szabad és tájékozott döntéshozatalra való képességét bármilyen módon befolyásolják.⁸⁰² Az interfészek kialakításának ez a megközelítése hasonló elvet követ,

⁷⁹⁶ BEUC: „Dark Patterns” and the EU Consumer Law Acquis: Recommendations for better enforcement and reform. 2022. 11. [beuc-x-2022-013_dark_patterns_paper.pdf](#) (letöltés: 2023. 11. 03.)

⁷⁹⁷ A sötét megoldásokkal kapcsolatos rendelkezések a 3. szakaszban, Az online platformot üzemeltető szolgáltatókra alkalmazandó további kötelezettségek című részben találhatók.

⁷⁹⁸ DSA (67) preambulumbekzdés

⁷⁹⁹ DSA (67) preambulumbekzdés

⁸⁰⁰ DSA (67) preambulumbekzdés

⁸⁰¹ DSA (68) preambulumbekzdés

⁸⁰² DSA 25. cikk (1) bekezdés

mint a GDPR beépített és alapértelmezett adatvédelem elvárása,⁸⁰³ tulajdonképpen mindkettő előre vágja el adott jogsértések lehetőségét. Ez azonban csak abban az esetben lehet hatékony a DSA-t illetően, ha körültekintően határozzák meg a sötét megoldások körét. A Bizottság iránymutatást fogalmazhat meg olyan interfészkialakításokra vonatkozóan, amelyek a következő három sötétmegoldás-típussal összefüggenek: választási lehetőségek kiemelése, ismételt felkérések (felugró ablak), megszüntetésre irányuló eljárás megnehezítése.⁸⁰⁴

A szakirodalom számtalan joghézagot és koherenciát érintő kérdést vetett már fel,⁸⁰⁵ nagyobb léptékekben gondolkodva azonban az érintett jogszabályok egymásra épülése annyiban vitathatatlan, hogy azok vagy feketelistával, vagy az online felület kialakítására vonatkozó, ún. interfészkialakítási rendelkezésekkel reagálnak a sötét megoldásokra. Az interfészkialakítási előírások a jogsértési lehetőségek megelőzésével kívánják minimalizálni a megoldásokat; a feketelista az utólagos szankció eszköze. Mindezek mellett is kérdés marad az, hogy a DSA-ben felsorolt gyakorlatok⁸⁰⁶ lefedik-e mindazon gyakorlatokat, amelyek nem tartoznak sem a GDPR, sem a UCP-irányelv hatálya alá, vagyis hogy a három uniós jogszabály együttesen képes-e a sötét megoldásokat kezelni.

Az európai adatgazdaság potenciális növelését szolgáló Data Act használja a sötét megoldások kifejezést, és definíciószerű elemeket is tartalmaz, amelyek – bár más szavakkal fogalmazva – ugyanazt a három jellemzőt emelik ki, mint tette azt a DSA: interfészmegoldásokhoz kötődnek; manipulatív, megtévesztő jellegűek; és ebből következően gyakorolnak negatív hatást a fogyasztói döntésekre.⁸⁰⁷ A Data Act esetében különösen fontos a sötét megoldások tiltása, hiszen az IoT-termékekből származó termékadatokat és a kapcsolódószolgáltatás-adatokat az adatbirtokos a felhasználó kérelmére harmadik fél rendelkezésére bocsáthatja, tehát az adatmegosztás három fél vonatkozásában bír jelentőséggel. Ebből következően sem az adatbirtokos (általában a gyártó), sem a harmadik fél nem nehezítheti meg indokolatlanul a felhasználó adatmegosztással kapcsolatos választási lehetőségeinek vagy jogainak a gyakorlását, mely magában foglalja a nem semleges módon kínált választási lehetőségeket éppúgy, mint az interfészmegoldásokat.⁸⁰⁸

⁸⁰³ GDPR 25. cikk, PETRÁNYI-DOMOKOS-HORVÁTH-HUSZÁR i. m. 19.

⁸⁰⁴ DSA 25. cikk (1) bekezdés és (3) bekezdés

⁸⁰⁵ PETRÁNYI-DOMOKOS-HORVÁTH-HUSZÁR i. m. 19–20.; PUSZTAHELYI Réka: *A személyes adatok üzleti célú megszerzésére alkalmazott „sötét minták” elleni fellépés lehetséges formái.* In *Medias Res* 2023/2. 158–161.; BEUC: *„Dark Patterns”* i. m. 11.

⁸⁰⁶ DSA 25. cikk (2) bekezdés

⁸⁰⁷ Data Act (38) preambulumbekkezdés

⁸⁰⁸ Data Act 4. cikk (4) bekezdés és 6. cikk (2) bekezdés a) pont, valamint a (38) preambulumbekkezdés

3. A digitális sérülékenység kezelése

A növekvő automatizmus miatt potenciálisan szinte minden átlagfogyasztót fenyeget a digitális aszimmetria és ebből következően a digitális sérülékenység, azaz bizonyos helyzetekben bárki kiszolgáltatottá válhat,⁸⁰⁹ ezért digitális környezetben az átlagfogyasztó és a kiszolgáltatott fogyasztó fogalmi már nem képesek funkciójukat teljes mértékben betölteni. A Fitness Check javaslata szerint az átlagfogyasztó fogalmának a fogyasztók valós viselkedésére és a digitális környezetben tapasztalható aszimmetriák miatt a további sebezhetőségekre kell vonatkoznia.⁸¹⁰

Goanta és szerzőtársai szerint nem célravezető az, hogy az átlagfogyasztó fogalmába új, specifikus sérülékenységi jegyeket illesszenek be; valamint a bírói gyakorlat is nagyszámú esetet és hosszú időt igényelne.⁸¹¹ A nagy online platformok esetében a jogi megoldásnak alapvetően a rendszerszemléletű megközelítéshez kell fordulnia. Mivel a DSA a platformok szabályozói képességét elismeri (pl. a jogellenes tartalmak kezelésében),⁸¹² a platformok felelősségére kell összpontosítani, oly módon, hogy a digitális sérülékenységgel kapcsolatban központi szerepet játszanak nemcsak a jogi standardok tartalmának átalakításában, hanem azok eljárási alkalmazásában is.⁸¹³ Ehhez alapot nyújtanak a különböző adatbázisok – így a DSA átláthatósági jelentési és indoklási kötelezettsége kapcsán létrejövő adatbázis (ami az online piactereket is érinti), valamint az általános termékbiztonságról szóló rendelet Safety Gate riasztórendszere –, amelyek szabályozási adminisztrációként foghatók fel, és könnyen implementálhatók a platformok architektúrájába, azzal az előnnyel, hogy automatizálhatók a megfelelési ellenőrzések is. Összegezve a digitális sérülékenység kezelésére a jogi normák rendszerszintű technikai beágyazása látszik a leginkább célravezetőnek a platformokon,⁸¹⁴ és szolgálhat útként a digitális méltánytalanságtól a méltányossághoz. Ennek a megoldásnak több kiemelkedő eleme van: a jogalkotók és a platformok együttműködését igényli; megelőző hatású, ezáltal hatékonyabb, mint az utólagos jogérvényesítést lehetővé tévő eszköz; valamint illeszkedik abba a folyamatba, amely a fogyasztóvédelmi szempontok gyári beállítását, beépítését preferálja, mint a GDPR beépített és alapértelmezett adatvédelem elvárása, a DSA

⁸⁰⁹ *Fitness Check i. m. 22.*; HELBERGER et al. *i. m. 25.*

⁸¹⁰ *Fitness Check i. m. 345.*

⁸¹¹ GOANTA–DE GREGORIO–SPANAKIS *i. m. 47.*

⁸¹² Tóth (2023) *i. m. 25.*; lényegében ugyanezt erősíti: MENYHÁRD Attila: *A platformok polgári jogi felelőssége*. In: TÖRÖK Bernát – ZÓDI Zsolt (szerk.): *Az internetes platformok kora*. Bp., Ludovika Egyetemi Kiadó, 2022. 132.: „Amikor a közösségi oldalak üzemeltetőjétől az alapjogok betartását várjuk el, akkor valójában állami feladat ellátását várjuk el tőle [...], a platformokat nem elegendő szabályozási tárgyként kezelni; eredményesebb megközelítés lenne [...] partnernek tekinteni, és erre felépíteni az [...] állami kontrollt.”

⁸¹³ GOANTA–DE GREGORIO–SPANAKIS *i. m. 49–51.*

⁸¹⁴ GOANTA–DE GREGORIO–SPANAKIS *i. m. 48–52.*

beépített megfelelés rendelkezése vagy a sötét megoldások tilalmára vonatkozó interfész kialakítási rendelkezések.⁸¹⁵

A kutatók megvizsgálták a UCP-irányelv digitális környezethez igazítási lehetőségét is – amely magában foglalná a tisztességtelen digitális kereskedelmi gyakorlatok feketelistáját, valamint a digitális kereskedelmi gyakorlat és a digitális szakmai gondosság fogalmának meghatározását is –, de felhívják a figyelmet arra, hogy valójában paradigmaváltásra van szükség, a fogyasztóvédelmi joggal kapcsolatos gondolkodásmód megváltoztatására, ami nem azonos a UPC-irányelv módosításával.⁸¹⁶

Ennek érdekében a fogyasztók sebezhetőségeit, sérülékenységet az EU a DFA jogszabállyal kívánja kezelni, ami tervek szerint azokra a problémákra reagál majd, amelyeket a Fitness Check tanulmány azonosított, és amelyek aláássák a fogyasztók védelmét: sötét megoldások, digitális szolgáltatások függőséget okozó kialakítása, tisztességtelen személyre szabás és profilalkotás, tisztességtelen árképzési taktikák, digitális szerződésekkel, előfizetésekkel és azok lemondásával kapcsolatos problémák, influenszerek félrevezető gyakorlatai.⁸¹⁷ Ezek nagyobb részét a fogyasztóvédelmi eszközrendszer már szabályozza, mégis számottevően érinti az európai fogyasztókat. A DFA-nek a UCP-irányelv digitális ikertestvéreként kell szolgálnia, mind horizontális struktúrája, mind az általános záradéklogika (feketelista-melléklet) tekintetében, miközben kiterjeszti hatókörét az algoritmusok generálta aszimmetriák kezelésére is.⁸¹⁸ Remélhetően alaptalanok azok az aggodalmak, amelyek szárnyra kaptak a DFA-vel kapcsolatban, nevezetesen, hogy csak javítás vagy módosításcsomag lesz. Az aggodalom oka az, hogy a parlamenti képviselők egy része nem támogat egy ambiciózus jogszabályt, mert a fogyasztóvédelmi szempontokon túl a versenyképesség, a növekedés előmozdítása is fontos annak érdekében, hogy az EU-ban is kialakuljanak nagy digitális vállalkozások, erre pedig csak a túlszabályozás elkerülésével van esély.⁸¹⁹

Fontos megjegyezni, hogy a platformok használatával összefüggésben a digitális sérülékenység nemcsak a fogyasztókat érinti, hanem tágabb kört, a polgárokat. Erre utal a DSA: „Különösen súlyos negatív hatásokkal járhat, ha a szolgáltatás igénybe vevői az érdeklődésüknek megfelelően optimalizált, célzott technikákon alapuló hirdetéseket látnak,

⁸¹⁵ GDPR 25. cikk, DSA 31. cikk és DSA 25. cikk

⁸¹⁶ Monika NAMYSŁOWSKA: *Future-Proofing the Unfairness Test*. In: Natali HELBERGER et al.: *Digital fairness for consumers*. 2024. 234. https://www.beuc.eu/sites/default/files/publications/BEUC-X-2024-032_Digital_fairness_for_consumers_Report.pdf (letöltés: 2025. 03. 02.)

⁸¹⁷ TAMIM (2025) i. m.

⁸¹⁸ NAMYSŁOWSKA (2025) i. m. 333.

⁸¹⁹ James TAMIM: *Will the Digital Fairness Act be a Regulation?* Hír, 2024. 12. 09. <https://digitalfairnessact.com/will-the-digital-fairness-act-be-a-regulation> (letöltés: 2025. 03. 02.)

amelyek potenciálisan gyenge pontjaikat használják ki. Bizonyos esetekben a manipulatív technikák egész csoportokra negatív hatást gyakorolhatnak, és felerősíthetik a társadalmi károkozást, például azáltal, hogy hozzájárulnak a dezinformációs kampányokhoz vagy megkülönböztetést alkalmaznak bizonyos csoportokkal szemben.”⁸²⁰ A DSA-ből – a digitális térben elfoglalt aktuális szerep, pozíció alapján – a digitális sebezhetőség szélesebb értelmezése bontakozik ki. A sebezhetőségek egy része a fogyasztókra, más része a polgárookra vonatkozik, vagyis a sérülékenységeknek társadalmi következményei is lehetnek.⁸²¹

4. Koherencia vagy széttöredezettség?

A fogyasztók védelme a személyes adataik kezelése tekintetében több klasszikus területen és több jogszabályban elszórva kap szerepet, ami azzal jár, hogy ugyanannak a problémának a kezelésében egyszerre több jogszabály releváns, de ezek nem ugyanúgy és nem ugyanazt szabályozzák. Az adatvédelem és a fogyasztóvédelem metszetében elhelyezkedő algoritmikus rangsorolás, dinamikus árképzés, sötét megoldások, személyre szabott reklámok, profilalkotás szabályozási rendszere emelhető ki példaként, ezek közül az utóbbi hármat vizsgálom, mert ezek többször is hangsúlyt kaptak dolgozatomban.

A sötét megoldások tilalmára vonatkozó szabályozás a DSA-ben és a UCP-irányelvben is helyet kapott. Míg a DSA használja a sötét megoldás kifejezést, a felhasználói felület kialakításával és manipuláló hatásával kapcsolatban szabályoz, és az online platformok bizonyos interfészalkakítására vonatkozóan konkrét tilalmat fogalmaz meg; addig a UCP-irányelv nem használja a kifejezést, a fogyasztói döntés torzítását szankcionálja minden kereskedelmi gyakorlat vonatkozásában, és csak általános tilalomkategóriákat tartalmaz.⁸²² Ez azt is jelenti, hogy eltérő hatóságok végezhetnek vizsgálatot, amelynek során akár különböző eredményre is juthatnak, ami akadályozza a védelem egységes, azonos szintű érvényesülését is. A különbségek – más fogalomkészlet, más a szabályozás célja, a végrehajtás stb. – azt mutatják, hogy a sötét megoldások kezelését a DSA és a UCP-irányelv is más logika alapján közelíti meg, így nem a koherenciát erősítő, hanem ellene ható tényezővé válnak.

A személyre szabott hirdetések tekintetében a fogyasztó védelmét több uniós jogszabály is szolgálja. Ezzel összefüggésben a GDPR meghatározza az adatkezelés jogszerű jogalapjait; az UCP-irányelv célja az, hogy a tisztességtelen kereskedelmi gyakorlatok ne manipulálják a

⁸²⁰ DSA (69) preambulumbekzdés

⁸²¹ Marijn SAX – Natali HELBERGER: *Digital Vulnerability and Manipulation in the Emerging Digital Framework*. 11–24. In: Natali HELBERGER et al.: *Digital fairness for consumers*. 2024. 13.

⁸²² DSA (67) preambulumbekzdés, 25. cikk; UCP-irányelv (13) preambulumbekzdés, 5–9. cikk

fogyasztó döntéseit; míg a DSA célja e hirdetések átláthatóságának biztosítása.⁸²³ Ez az eltérő célrendszer nem vezethet egységes értékeléshez sem: a személyre szabott hirdetés a GDPR szerint akkor jogszerű, ha megfelelő a jogalap; a UCP-irányelv alapján akkor jogszerű, ha nem torzítja tisztességtelenül a fogyasztói döntést; és a DSA szerint akkor jogszerű, ha átlátható. A jogszabályok különböző megközelítését jól példázza magának az átláthatóságnak a kérdése is. A GDPR alapján az adatkezelési tájékoztatóhoz kapcsolódva részletesen kell tájékoztatni az érintettet az adatkezelés céljáról, időtartamáról stb.; a UCP-irányelv kulcsfontosságú információkat határoz meg, amelyekre a fogyasztónak szüksége van a tájékozott döntés meghozatalához; a DSA pedig magának a hirdetésnek az átláthatóságát várja el.⁸²⁴ Egyetlen szempont és mégis eltérő tartalmú és szintű az elvárás. Érdeemes még a felhasználói kontroll lehetőségét is megvizsgálni a személyre szabott hirdetésekkel kapcsolatban. A GDPR a tiltakozás jogát biztosítja, ill. kártérítéshez való jogot is; a UCP-irányelv nem ad a fogyasztó kezébe kontrollt, ezek az irányelv tilalmába foglalva jelennek meg, de jogorvoslati lehetőséget tartalmaz; a DSA információt ad a célzásról, ahogy az átláthatóságnál említettük, valamint kártérítés kérhető az elszenvedett kárért.⁸²⁵ Mindezek azt bizonyítják, hogy a joggyakorlásnak sem azonosak a lehetőségei. Mivel a szempontok különbözőek, és ezek ellenőrzése sem ugyanazon szervek hatáskörébe tartozik, így az eredmény és a szankció is lehet különböző. A különböző szempontok és az egymás mellett párhuzamosan futó értékelések a koherencia ellen, ezzel együtt a védelem egységessé ellen hatnak.

A profilozásra vonatkozóan szintén a GDPR, a UCP-irányelv és a DSA releváns. A személyre szabott hirdetések profilalkotáson alapulnak, a profilt a hirdetésekhez, célzásokhoz használják fel. Ezzel magyarázható az, hogy ami az előzőekben, az említett hirdetésekkel kapcsolatban a szabályozás céljára, jogszerűségére, átláthatósági követelményeire és a felhasználói kontrollra vonatkozóan megállapításra került, ugyanaz elmondható a profilalkotásra vonatkozóan is. Különbség csupán néhány van, de azok jelentősek. A profilalkotás önálló adatkezelési művelet, ezért a GDPR önálló fogalomként és külön cikkekben szabályozza; a személyre szabott hirdetés pedig csupán a profil felhasználási területe. A UCP-irányelv és a DSA nem nevesíti a profilalkotást, előzőben csak közvetetten jelenik meg, utóbbiban pedig az ajánlórendszerek részeként.⁸²⁶ Az automatizált döntéshozatal is olyan szempont, amely különbségeket mutat. A profilalkotás a GDPR-ban központi kérdés,

⁸²³ GDPR 6. cikk; UCP-irányelv 5–9. cikk; DSA 26. cikk, 39. cikk

⁸²⁴ GDPR 13–14. cikk; UCP-irányelv 14. cikk; DSA 26. cikk, 39. cikk

⁸²⁵ GDPR 21. cikk, 79. cikk, 82. cikk; UCP-irányelv 11. cikk; DSA 54. cikk

⁸²⁶ GDPR (71) preambulumbekzdés, 4. cikk 4. pont, 22. cikk; UCP-irányelv 5–9. cikk; DSA 3. cikk s) pont, 27. cikk

ezért önálló cikk szabályozza; de mivel nem minden hirdetés eredményez jelentős joghatást, ezért az automatizált döntéshozatal szempontjából nem válik központi kérdéssé; a UCP-irányelv nem szabályozza; a DSA pedig csak az algoritmusok működésén belül érinti.⁸²⁷ A profilalkotás adatvédelmi kockázatot hordoz, ezért a GDPR-ban adatvédelmi hatásvizsgálatot igényel; a hirdetés a fogyasztói magatartásra vonatkozóan hordozhat kockázatot, ezért a DSA-ban rendszerszintű kockázatértékelést igényel; a UCP-irányelv nem rendelkezik erre vonatkozóan.⁸²⁸

A vázolt koherenciaproblémák arra is rámutatnak, hogy mindhárom terület az adatvédelem (GDPR), a manipuláció (UCP-irányelv) és a platformok (DSA) működésének összefüggésére épül; s minél több az érintett jogszabály, annál erősebb a koherenciahiány. Bár a sötét megoldásokkal kapcsolatban csak két jogszabályt vetettem össze, ezek mégis olyan problémakört jelentenek, amelyek digitális környezetben kapcsolódnak a személyes adatok kezeléséhez. (A 7. táblázat több jogszabályhelyre rámutat.) A sötét megoldások, a személyre szabott hirdetések és a profilalkotás vizsgálata alapján leszűrhető az a következtetés, hogy a szabályozás nem a koherencia, hanem a széttöredezettség, a fragmentáció irányába hat. Különösen szembeűnő ez a személyre szabott hirdetések és a profilalkotás tekintetében, mert egymással összefüggő és egymást feltételező fogalmakról van szó: adatkezelési műveletről és annak egyik felhasználási területéről; mégis más a megközelítés és a szabályozás logikája.

A koherenciaproblémák minden szereplő számára hátrányosak. A vállalkozásoknak nehéz megítélni, hogy üzleti modelljük melyik jogszabály hatálya alá tartozik, és melyik hatóság fog eljárni (pl. az adatvédelmi hatóság a GDPR alapján, vagy a digitális szolgáltatási koordinátor a DSA alapján, vagy a hagyományos fogyasztóvédelmi hatóság a UCP-irányelv alapján). Azon túl, hogy az uniós piacon 27 különböző nemzeti fogyasztóvédelmi jogszabálynak is meg kell felelni, az adminisztratív terhek növelik az információs-technológiai és a jogi megfelelési költségeket. A fogyasztó szempontjából szintén nehéz kibogozni, hogyan érvényesítheti a jogait. A jogalkalmazóknak és a hatóságoknak sem egyszerű feladat a hatásköri határok kijelölése (az említett koordinátor és a hagyományos fogyasztóvédelmi hatóságok között) és a hatékony együttműködés megteremtése. Számolni kell azzal is, hogy a digitális szolgáltatások és az algoritmusok szabályozása olyan mély jogi és technikai szakértelmet igényel a hatóságoktól, ami nem mindig áll rendelkezésre, ez pedig lassítja a hatékony fellépést a jogsértésekkel szemben. A különböző jogszabályok eltérő harmonizációs szintje nehezíti az EUB és a nemzeti bíróságok számára az egységes ítélkezési gyakorlat kialakítását is.

⁸²⁷ GDPR 22. cikk; DSA (68)–(70) preambulumbekzdés

⁸²⁸ GDPR 35. cikk; DSA 34–35. cikk

Mi mozdítaná előre a koherenciaproblémák csökkentését? Az egyik elmozdulási irány – véleményem szerint – az egységes fogalomrendszer használata jelentené. Például a profilalkotás fogalmat csak a GDPR használja, a DSA és a UCP-irányelv nem. Utóbbiak csak a profilalkotásra mint funkcióra utalnak: tudjuk, hogy a profilalkotás szerepe a befolyásolás, és a UCP-irányelv szintén tartalmazza a befolyásolást, de gazdasági téren: („torzíthatja vagy torzíthatja azon átlagfogyasztó gazdasági magatartását”); a DSA-ben a profilalkotás funkcióját a rangsorolás, a paraméterek hordozzák („a szolgáltatás hirdetéssel megcélzott igénybe vevőjének meghatározására szolgáló paraméterekkel”), ill. egy alkalommal nevesítve is szerepel (a kiskorúakra vonatkozó profilalkotás tilalma).⁸²⁹ Az egységes fogalomhasználat elősegítené a profilalkotás megközelítését a felsorolt jogszabályokban. Ugyanígy szükséges lenne a sötét megoldások és a személyre szabott hirdetések fogalmának egységes definiálása. Alkalmas keretet biztosíthat erre a készülő DFA. A széttöredezettség csökkentését eredményezné a végrehajtásban érintett szervezetek együttműködési kereteinek kidolgozása, valamint közös iránymutatások készítése is előrevinné az egységes megközelítést.

5. Sajátos szabályozási terület születőben – fogyasztóvédelmi adatjog?

Hipotézisem szerint sajátos szabályozási terület van kialakulóban, ami fogyasztóvédelmi adatjognak nevezhető. Annak érdekében, hogy a hipotézist bizonyítsam, avagy cáfoljam, a továbbiakban összegzem azokat a fogyasztóvédelmi jogszabályokat, amelyek a fogyasztókat adatvédelmi rendelkezésekkel is védik. Ezt követően számbaveszem azokat a kritériumokat, amelyek meghatározók a szabályozási terület önállóságának megítélésében, valamint a fogyasztóvédelmi jog koherenciaproblémái felől is megvilágítom a kérdést.

Az EU hagyományos fogyasztóvédelmi eszközrendszere – a klasszikus területeken, mint például a szerződési feltételek vagy a kereskedelmi gyakorlatok szabályozása – nem tartalmazott konkrét rendelkezéseket a fogyasztók személyes adataival összefüggésben; eleinte csupán az offline piacokra vonatkozó tilalmakat és rendelkezéseket alkalmazták az online piacokon is, de konkrétan a fogyasztók személyes adatainak védelmével kapcsolatban a fogyasztóvédelmi jog nem sokat tett.⁸³⁰ Ez azt jelenti, hogy a fogyasztóvédelem és az adatvédelem sokáig két külön világot alkotott, de – a technológiai fejlődés rohamos üteme révén megjelenő kihívások miatt – ma már nem beszélhetünk egymástól merőben elkülönülő

⁸²⁹ UCP-irányelv 5. cikk (2) bekezdés b) pont; DSA 26. cikk (1) bekezdés d) pont, 28. cikk (2) bekezdés

⁸³⁰ Rong HAN – Na JIANG: *The integration of personal data protection into consumer law in EU digital markets*. Journal of Legal, Ethical and Regulatory Issues 2024/27. 1–6. <https://www.abacademies.org/articles/the-integration-of-personal-data-protection-into-consumer-law-in-eu-digital-markets-16802.html#r4> (letöltés: 2025. 11. 05.)

területekről. A fordulópontot a 2019. évi DCS-irányelv jelentette, amely szerződésszerű jogokat adott a fogyasztóknak, kikötve, hogy ez a GDPR-al összhangban történhet. Még ugyanebben az évben az omnibusz irányelv illesztett be adatvédelmi rendelkezéseket a klasszikus fogyasztóvédelmi jog uniós normáiba – felismerve, hogy a fogyasztóvédelem szerves részét kell képezze a fogyasztók adatainak védelme –, majd 2022-től (DSA) felgyorsult és intenzívebb lett ez a folyamat. A fogyasztóvédelmi jogszabályokban megjelent adatvédelmi rendelkezéseket összegzi a 8. táblázat.

8. táblázat: Fogyasztóvédelmi jogszabályok adatvédelmi rendelkezései

JOGSZABÁLY	TÁRGY	NEVESÍTETT ADATVÉDELMI RENDELKEZÉSEK
UCT-irányelv (1993)		
UCP-irányelv (2005)		
CR-irányelv (2011)	tájékoztatás	automatikus döntéshozatal alapján személyre szabott-e az ár [6. cikk (1) bek. ea) pont] – az omnibusz irányelv illesztette be 2019-ben
DCS-irányelv (2019)	digitális tartalom szolgáltatására... irányuló szerződés: személyes adat = 'ellenszolgáltatás'	- személyesadat-kezelés a GDPR és az elektr. hírközl. adatvéd. irányelv alapján [(37) preamb.] - megegyeztet: - személyesadat-kezelés jogszervi jogalap alapján [(24) preamb.] - adathordozhatóság, hozzájárulás visszavonása [(38)–(39) preamb.] - GDPR adatkezelési elvek megsértése → hibás teljesítés [(48) preamb.]
képviselési keretokról szóló irányelv (2020) I. melléklete	képviselési kereset indítása	- fogyasztóvédelmi jog – adatvédelem tekintetében történő – hatékonyabb érvényesítése érdekében [(13) preamb.] - GDPR és elektr. hírközl. adatvéd. irányelv rendelkezéseinek megsért. esetén [I. mell. 10., 56. p.]
DSA (2022)	- profilalkotáson alapuló hirdetések megjelenítése online platformok számára - kockázateértékelés VLOP, VLOSE számára	- gyerekek számára tilos [28. cikk] - személyes adatok különleges kategóriáinak felhasználásával tilos [6. cikk (3) bek.] - szempontja a személyes adatok védelméhez való jog } [34. cikk (1) bek. b) pont] - szempontja a gyermekek védelméhez való jog }
általános termékbiztonságról szóló rendelet (2023)	- összekapcsolt termékek értékelési szempontja - biztonság	- adatvédelmi előírások a gyermekek érdekében [(23) preamb.] - gyűjtött személyes adatok minimalizálása [35. cikk (2) bek.]
fogyasztói hitelmegállapodásokról szóló irányelv (2023)	hitelképesség-vizsgálat	- tájékoztatás: automatizált döntéshozatalról [(46) preamb.] - adattakarékosság, pontosság, célhoz kötöttség [(30) preamb.] - személyes adatok különleges kategóriáinak felhasználási tilalma [(55) preamb.]
termékfelelősségi irányelv (2024)	kártérítéshez való jog	szoftver (=termék) által okozott kár: nem szakmai célokra használt adatok megsemmisülése, sérülése esetén (a GDPR megsértésére nem vonatkozik) [6. cikk (1) bek. c) pont]

Forrás: saját szerkesztés a táblázatban szereplő jogforrások alapján

A táblázat megerősíti, hogy adatvédelmi rendelkezések gyakran szivárognak át a fogyasztóvédelmi keretekbe, a fogyasztó védelme az adatkezelés szabályozásán keresztül is megvalósul. Ennek legfőbb oka az, hogy a GDPR önmagában nem feltétlenül védi teljes mértékben a fogyasztó személyes adatait, mert a fogyasztóvédelmi jogszabályoktól függetlenül működik.⁸³¹ A fogyasztót már nemcsak a hagyományos aszimmetria ellen kell védelemben részesíteni, hanem a digitális környezetben a sérülékenységgel szembe, ahol személyes adatait algoritmusokkal dolgozzák fel, profilt készítenek róla, és ezek alapján döntést hoznak róla. A klasszikus fogyasztóvédelmi modellhez képest ez sokkal mélyebb megközelítés, és illeszkedik

⁸³¹ Rong HAN – Na JIANG: *The integration of personal data protection into consumer law in EU digital markets*. Journal of Legal, Ethical and Regulatory Issues 2024/27. 1–6. <https://www.abacademies.org/articles/the-integration-of-personal-data-protection-into-consumer-law-in-eu-digital-markets-16802.html#r4> (letöltés: 2025. 01. 02.)

abba a folyamatba, hogy a GDPR szabályai „horizontális jelleggel türemkednek be több jogterület szabályai közé.”⁸³²

A további bizonyításhoz számba kell venni a szabályozási területek legfontosabb elemeit: ki a jogalany, van-e saját fogalomrendszere, és milyen intézményrendszere van. Ezek közül a jogalanyiség a kulcskérdés. Az adatvédelmi jog alanya az érintett, a fogyasztóvédelmi jogé a fogyasztó, a fogyasztóvédelmi adatjognak azonban nincs önálló alanya. Ahogy az érintett és a fogyasztó kapcsolatának értelmezésénél rámutattunk, e kettő metszetében a digitális szolgáltatást igénybe vevő fogyasztók, rövidebben fogalmazva a digitális fogyasztók (más szóval online fogyasztók) helyezkednek el, ez azonban nem önálló jogi kategória, jelenleg egyetlen uniós jogszabály sem használja, így definíciója sem létezik. Az érintetti státusz nem fogyasztói minőséghez kötött, és a fogyasztói helyzet nem jelent automatikusan adatkezelést. Ez összefüggésbe hozható a védelem céljával – ahogy az érintetti és a fogyasztói alanyi kör összehasonlítása során láttuk (3. táblázat) –, a védelem jellege a GDPR érintettjére vonatkozóan alapjogi, a fogyasztóvédelmi jogszabályok fogyasztójára vonatkozóan pedig gazdasági jellegű.

A saját fogalomrendszert mint követelményt illetően – visszautalva dolgozatom fogalmakat értelmező fejezetére – azt láttuk, hogy mind az adatvédelem fogalmai (személyes adat, érintett stb.), mind a fogyasztóvédelem fogalmai (fogyasztó, kereskedő stb.) körülhatárolhatók, s a rendelkezések e fogalmakra vonatkozóan fogalmazódnak meg. S noha a fogyasztóvédelem fogalmait használják a digitális környezetben, új, speciális kategóriák nem jöttek létre. Egy példával szemléltetve: a pénzbeli ellenérték nélküli szerződés a jelenleg hatályos jogforrásokban még nem jelent új jogintézményt, hanem a szerződésszerűség és a GDPR metszetében értelmezhető. Továbbá az érintetti jogok (törlés, tiltakozás stb.) teljes egészében nem feleltethetők meg a fogyasztói jogoknak (elállás, szavatosság stb.), még ha közös elemeik vannak is (pl. a tájékoztatás), és ha az érintetti jogok sok esetben fogyasztóvédelmi analógia alapján születtek is.

A harmadik szempont, amit vizsgálni kell, az önálló intézményrendszer megléte. Ebből a szempontból az adatvédelemhez az adatvédelmi hatóságok, az EDPB stb., a fogyasztóvédelemhez a fogyasztóvédelmi hatóságok, a kollektív keresetek stb. kapcsolódnak. A fogyasztóvédelmi adatjoghoz nem kapcsolódik önálló intézményrendszer, adatvédelmi kérdésekben az adatvédelmi hatóság, tisztességtelen kereskedelmi gyakorlatok tekintetében a fogyasztóvédelmi hatóság, bizonyos esetekben a Bizottság jár el.

⁸³² HAJNAL Zsolt: *A digitalizáció hatása a fogyasztóvédelmi jogalkotásra*. Fontes Iuris 2024/3–4. 47. <https://doi.org/10.51784/FI.2024.3-4.5> (letöltés: 2025. 07. 20.)

A fogyasztóvédelmi adatjog önállóságának megítélésében a koherenciaproblémáknak is jelentősége van. A fogyasztóvédelmi jog széttagozott, a jogszabályok nem alkotnak egységes és koherens rendszert – ahogy az előző alfejezet rámutatott –, ugyanazt a magatartást több jogterület is szabályozza, de eltérő logikával. Ebből a tényből két következtetés vonható le. Egyrészt – mivel nincs közös fogalomrendszer, nincs közös ellenőrzési és végrehajtási rendszer, más a megközelítés stb. – a fogyasztóvédelem és az adatvédelem metszéspontjának szabályozására még nem alakult ki új jogterület, azaz nem beszélhetünk fogyasztóvédelmi adatjogról. Másrészt – mivel a széttagoltság felszámolhatóságához hozzájárulna – a fogyasztók védelme érdekében szükséges lenne a fogyasztóvédelmi és az adatvédelmi rendelkezéseket egységes keretbe foglalni, ez lehetne a fogyasztóvédelmi adatjog.

Mindezek alapján – de különösen a jogszabályi védelem jellege és az elkülönült jogalanyiség hiánya miatt – nem beszélhetünk sajátos szabályozási területről, tehát cáfolni kell azt a hipotézisemet, hogy kialakulóban lenne a fogyasztóvédelmi adatjog. Valójában a fogyasztóvédelem és az adatvédelem metszéspontjáról beszélhetünk, amit a digitális környezet indukált, és eredményeként megfigyelhető az a folyamat, hogy a fogyasztóvédelmi szabályokra adatvédelmi rendelkezések rétegződnek. A 8. táblázatban felsorolt jogszabályok mind fogyasztóvédelmi jellegűek, és a digitális környezet miatt a gyengébb fél védelmét adatvédelmi eszközökkel egészítik ki és erősítik meg, ezáltal a GDPR a fogyasztóvédelmi jogszabályokban realizálódik.

A szakirodalom alapvetően állást foglalt az adatvédelem és a fogyasztóvédelem összefüggése mellett, sőt a „data consumer law” (‘adatokhoz kapcsolódó fogyasztóvédelem’) gondolata is feltűnt már, amely a szerzői érvelés szerint azt jelenti, hogy a digitális gazdaságban az adatvédelem és a fogyasztóvédelem kezd összefonódni, ugyanakkor az integrált jövőképnek egyelőre akadályai vannak.⁸³³

Szerintem jelenleg olyan átmeneti időszakban vagyunk, amikor elmozdulás látszik abba az irányba, hogy a digitális (online) fogyasztó fogalma valóban körvonalazódik egyes jogszabályokban. A 8. táblázat alapján a digitális (online) fogyasztó fogalmához három elemet lehet azonosítani: online platformokkal összefüggésben, automatizált döntésekhez kapcsolódóan és a manipuláció elleni védelem alapján értelmezhető. Mindemellett e fogalom definiálása és bevezetése a fogyasztóvédelmi célú jogszabályokba nem várható, mert az aszimmetrikus viszonyok ellen az offline és az online világban a fogyasztót ugyanolyan védelem illeti meg. A jogalany ugyanaz, tehát fogyasztó; a digitális környezet adta helyzet más,

⁸³³ HELBERGER–BORGESIU–REYNA i. m. 1–2., 24. (pdf)

ezt azonban különböző eszközökkel kezeli. A digitális fogyasztó kirajzolódott fogalmi jegyei összefüggést mutatnak a digitális sérülékenység jelentésével, ehhez kapcsolódó jogalkotási eljárás jelenleg van folyamatban (DFA).

6. Összegzés és a fogyasztóvédelemben rejlő lehetőségek a jövőre vonatkozóan

A uniós fogyasztóvédelmi eszközrendszer elemei több jogszabályban vannak lefektetve. A UCT-irányelv melléklete nem tartalmaz a digitális piacokra vagy a platformokra vonatkozó utalást, a platformok működésével összefüggő új típusú tisztességtelen feltételt. Véleményem szerint ezek feltérképezése és beépítése a jogszabályba elősegítené azon ügyek megoldását, ahol a platformok az általános szerződési feltételek mögé bújva sértik meg a GDPR rendelkezéseit.

A DCS-irányelv a fogyasztói jogokat erősíti azzal, hogy digitális tartalom vagy szolgáltatás nyújtására irányuló szerződések keretében a fogyasztóknak ugyanolyan jogokat biztosít, mint a visszterhes szerződések esetében. Ennek érdekében az irányelv elismerte az olyan szerződéseket, amelyek alapján a fogyasztó személyes adatokat ad át, de anélkül, hogy árúnak vagy ellenszolgáltatásnak nevezné azokat. Egyetértek az alapjogi érvekkel, mégis úgy gondolom, hogy megfontolásra érdemes lenne az adat mint ellenszolgáltatás típusú szerződés fogalmának definiálása, mert nemcsak a szerződő felek egyensúlyát biztosítaná, hanem csökkenteni tudná a szolgáltatások devalválásának problémáját is.

A sötét megoldások kezelése érdekében szükséges lenne egységes definíció rögzítése, felhasználva a már több jogszabályban meglévő, definíciószerű elemeket is. A leendő definíció helyet kaphatna a tervezett DFA-ben, mert a sötét megoldások a digitális sérülékenység egyik okát jelentik. Egyetértve Namysłowska véleményével, a digitális szakmai gondosság érvényesülése érdekében egyrészt kifejezetten a digitális környezetben megjelenő tisztességtelen és agresszív gyakorlatok, így a manipuláció, az algoritmusok okozta hatások ellen általános tilalom beépítése szükséges a jogszabálcikkekbe; másrészt olyan feketelista létrehozása,⁸³⁴ amely a konkrét tilalmakkal nemcsak megkönnyítené, hanem gyorsítaná is a jogalkalmazók munkáját. Mind a fogalom meghatározásával, mind az általános tilalommal, mind a feketelista-melléklettel a DFA lehetne a koherenciát biztosító keretjogszabály, és mindazon manipulatív gyakorlatok kezelésére fókuszálna, amelyeket a DSA nem szabályoz. Ezt a célt csak abban az esetben tudja elérni, ha a DFA nem irányelv lesz, hanem rendelet.

⁸³⁴ NAMYSŁOWSKA (2025) *i. m.* 329–332.

Jelenleg még nincs jogalkotási javaslat, csupán koncepció létezik, a kapcsolódó nyilvános konzultáció már lezajlott.

A DSA-ban – véleményem szerint – szükséges lenne a kiskorúak személyes adatait felhasználó, profilalkotáson alapuló hirdetések tilalmát kiterjeszteni minden online közvetítő szolgáltatóra, mert ezzel a GDPR és a DSA erősebb koherenciája valósulna meg. Ugyanígy egységes tilalomért kiált a személyes adatok különleges kategóriáit felhasználó, profilalkotáson alapuló célzott reklámozás, ami egyelőre szintén csak az online platformok számára tilos.

Az említett javaslatok nagy lépést jelentenének a koherencia irányában és a fogyasztóvédelmi jog széttagozottságának felszámolásában. Elindíthatnak egy olyan irányt, amely kevesebb uniós jogszabályban lenne képes szabályozni a fogyasztói adatok védelmét, ezáltal koherensebb keretet alkotni. E szabályozás gerince a GDPR, a UCP-irányelv és a DSA lenne, ezek rendelkezéseit helyezné egységes fogalomrendszerbe és megközelítésbe a tervezett DFA.

VII. FEJEZET: ÖSSZEGZŐ GONDOLATOK, KÖVETKEZTETÉSEK

1. Tisztában vannak-e a felhasználók a személyes adataik értékével, gazdasági értéké válásának folyamatával, valamint hogy a GDPR által biztosított átlátható tájékoztatáshoz való jog segíti-e őket tájékozott döntést hozni a személyes adataik kezelésével kapcsolatban, képes-e az információs aszimmetriát ellensúlyozni?

A személyes adatok értékének megértéséhez közelebb visz, ha tudjuk, hogy a platformok hogyan jutnak a big data birtokába, azt mire és hogyan használják fel. A felhasználók gyakran maguk bocsátják rendelkezésre adataikat, más esetben a platformok szerzik meg, például a cookie-k elhelyezésével, de a jogalapok közül a hozzájárulás és a jogos érdek is szóba jöhet. Az adathalmaz önmagában nem értékes, azt kezelni kell, amelynek célja az, hogy a felhasználók viselkedését megfigyeljék, profilalkotással személyes jellemzőiket értékeljék, előre jelezve a várható magatartásukat, preferenciáikat. A kapott értékek alapján szabják személyre a reklámokat, és célozzák a felhasználókat, így monetizálva a személyes adatokat. Bár a profilalkotás hordozhat előnyöket a felhasználók számára, de jellemzően inkább veszélyeket hordoz, mert csoportokba sorolják őket, kihasználják gyengeségeiket, befolyásolják döntéseiket. E folyamatok többnyire rejtve maradnak a felhasználók előtt.

A személyes adatok kezelése és marketingcélú felhasználása tekintetében a két fél tudása nem azonos. A platform technológiai és jogi értelemben lényegesen több információval rendelkezik, mint a felhasználó, ami – a fogyasztóvédelemből ismert fogalommal leírva – információs aszimmetriához, egyensúlyhiányhoz vezet. Ennek kiegyenlítése érdekében a jogalkotó az adatkezelőtől átlátható adatkezelést és tájékoztatást vár el, az érintett számára az ehhez való jogot biztosítja, amely az adatvédelmi tájékoztatóban ölt testet. Az érintett, a felhasználó ez alapján hozhat tájékozott döntést arról, hogy beleegyezik-e személyes adatai kezelésébe, s ha igen, milyen mértékben. Meg kell állapítani – egyetértve Edwards–Veale és Waerdt véleményével –, hogy az online platformok tekintetében a beleegyezés leértékelt valutává vált; az információs aszimmetriát a GDPR nem képes kezelni, nem tudja felszámolni a platformok és a felhasználók közötti szakadékot, ezáltal inkább rögzül az aszimmetria, mintsem megszűnne. Azért nem képes kezelni, mert nem veszi figyelembe a platformok adatgyűjtésen és az adatok monetizálásán alapuló üzleti modelljét, valamint azokat a technológiákat, amelyeket a személyes adatok kezelése során alkalmaznak (profilalkotás, algoritmusok), ugyanakkor a GDPR az érintett felhasználókra terheli a felelősséget, akik a gyakorlatban döntési kényszerhelyzetbe kerülnek. Ebből ered az információs önrendelkezési

jog paradoxona: a szabályozás az egyéni döntési szabadságot hangsúlyozza, miközben maga az önrendelkezési jog okoz döntési dilemmát a felhasználók számára. A helyzetet tovább súlyosbítja az adatvédelmi tájékoztatók kezelhetetlen mennyisége, az információk terjedelme, olvasási időigénye, érthetetlen jogi nyelvezete, ami összefüggésbe hozható azzal is, hogy az adatkezelők célja nem az érintettek segítése, hanem önmaguk jogi védelmének biztosítása, ami az elszámoltathatóság követelménye alapján érthető is. Mindezek elvezetik a felhasználókat ahhoz a magatartáshoz, hogy szinte automatikusan kattintanak az elfogadás gombra. Álláspontom szerint ez a hozzáállás csak megnevezés szerint magatartási probléma, valójában adekvát viselkedés és „válasz” az információs aszimmetriából fakadó helyzetre, s miután a viselkedés beleegyezés-fáradtsággá állandósult, a döntés és a beleegyezés ma már inkább teher, mint jog.

Megoldásként szóba jöhet: a nyelvi egyszerűsítés; a tagolt, táblázatba rendezett információk; a beépített egyszerű választási lehetőségek kínálása; valamint az adatvédelmi ikonok használata. Véleményem szerint, ha a GDPR bevezetésével párhuzamosan vagy kevéssel ez után rendelkezésre álltak volna a digitális környezethez eleve adekvát adatvédelmi ikonok – amihez azonban még ma is hiányzik a széles körű kutatói támogatás, a szabványok és a Bizottság felhatalmazáson alapuló jogi aktusa –, akkor jelentős segítséget nyújthattak volna az érintettek számára. Az adatvezérelt vállalatok esetében azonban korlátozottan hatékonnak gondolom a felsorolt megoldásokat, mert már rögzült a beleegyezés-fáradtság. Az információs aszimmetria felszámolásához új módszerre, radikálisabb megközelítésre van szükség, amely egyszerűbb kommunikálást tesz lehetővé, például a felhasználó előre beállíthatná az eszközén, hogy a felhasználói viselkedés megfigyeléséhez mely felületeken járul hozzá, és melyeken nem.

A vázolt háromszereplős láncban a felhasználók tehát egyelőre nem tudják megoldani az aszimmetrikus helyzetet; a platformok nem akarják; a jogalkotók nem számoltak a felhasználói oldallal, nem vették figyelembe a GDPR megalkotása során az átlagos érintettől, az átlagfelhasználótól elvárható informáltságot és magatartást. A felhasználó aszimmetrikus tudásával szemben az adatkezelő helyzete is végiggondolható a GDPR alapján. Megállapítható, hogy a jogalkotó rengeteg követelményt és szabályt telepít az adatkezelőre, de ha az maximálisan megfelel a GDPR elvárásainak, és ezt bizonyítani is tudja, akkor a technológiai-jogi tudással bíró adatkezelői pozíció védelme megvalósul, ám ahogy láttuk, a felhasználói pozíció védelme, csak elvileg. Ez azt jelenti, hogy a GDPR-ban a jogalkotói szándék szimmetrikusan kezeli az adatkezelő és az érintett védelmét, de nem jelenti azt is, hogy a GDPR elvárásainak mindkét fél azonos mértékben tud megfelelni az információs aszimmetria miatt.

A személyes adatok gazdasági értékének vizsgálata alapján leszögezhető, hogy – az adatgyűjtés, a profilalkotás, a cookie-k, az adatkezelési információk mennyisége és terjedelme, az információs aszimmetria miatt – egyre mélyebb a szakadék a platform és a felhasználó között, utóbbiak egyre kevésbé tudnak tájékozott döntést hozni, és ezáltal alanyaivá válnak a személyre szabott hirdetéseknek. Ezen a helyzeten a DMA rendelkezései sem segítenek, mert a kapuőrök számára nyitva hagyja az utat az adatkezelésre és keresztfelhasználásra, ha megszerzik a felhasználó hozzájárulását, s ezáltal az ördögi kör újra indul.

A személyre szabott hirdetésekkel szemben többféle védelmi mechanizmus áll rendelkezésre. A GDPR intézményei megfelelő védelmi szintet biztosítanak a felhasználóknak, ezt azonban lerontja az információs aszimmetria. Ellensúlyt jelent az is, hogy mind a profilalkotáshoz, mind a targetált hirdetésekhez kapcsolódóan garanciákat nyújt a jogalkotó a felhasználó számára (tiltakozáshoz és tájékoztatáshoz való jog), ill. hogy a védelemnek ki kell terjednie a harmadik országba történő adattovábbításra is. További megoldásként merült föl a hozzájárulást vagy díjfizetést megkövetelő modell alkalmazása, amely azonban a kibocsátott EDPB-vélemény és a Bizottság vizsgálata alapján sem reális alternatíva. A védelmi háló felsorolt elemei mellett annak is jelentősége van, hogy a felhasználó, a fogyasztó tud-e ellene védekezni. Vannak olyan ágazatok, ahol a profilalkotás és a célzott reklámok negatív hatásait képes kivédeni körütekintő, tudatos magatartással. Vannak azonban olyan területek, ahol a reklámok hatása ellen tud, de a profilalkotással járó következmények ellen nem tud védekezni, jellemzően idetartoznak a pénzügyi szolgáltatások.

Végkövetkeztetésem megfelel az előzetes várakozásomnak: *A felhasználók nincsenek tisztában személyes adataik értékével, mert nem látják át teljes egészében a nagy platformok üzleti modelljét. A GDPR által biztosított átlátható tájékoztatáshoz való jog és az adatkezelési tájékoztató ugyan elvileg lehetőséget ad a tájékozott döntés meghozatalára az adataik kezelését illetően, valamint az információs aszimmetria feloldására; a gyakorlatban azonban csupán formális szerepet töltenek be, tehát nem képesek felszámolni az egyensúlyhiányos helyzetet.*

2. Milyen mértékben képes a GDPR rendeletjellege és területi hatálya biztosítani az érintettek egységes védelmét az EU-ban, különös tekintettel a fogalomrendszer alkalmazhatóságára, az adatkezelési alapelvek érvényesülésére, az érintetti jogokra és a végrehajtás kérdéseire; valamint megfelelő védelmi szintet biztosít-e az elektronikus hírközlési adatvédelmi irányelv a felhasználók számára?

A GDPR jogszabálytípusa garancia arra, hogy egységes védelmet biztosítson az érintettek számára, s csak néhány területen enged teret a tagállami szabályozásnak, ide tartoznak a levéltárak archiválásra és hozzáférésre vonatkozó nemzeti szabályai, vagy az információs szolgáltatásokkal összefüggésben a hozzájárulás érvényességéhez szükséges életkor meghatározása. Az érintetti érdekek megkövetelték a területi hatály extraterritoriális kiterjesztését, azaz a tevékenységi hellyel rendelkező és nem rendelkező adatkezelőre is alkalmazni kell, utóbbi esetben nemcsak áruk és/vagy szolgáltatások nyújtásához, hanem az érintettek viselkedésének megfigyeléséhez is kapcsolódhatnak az adatműveletek. Értéke az, hogy a tengerentúli adatkezelők és a marketingcélú hirdetések vonatkozásában is védelmet biztosít az érintettek részére.

Az adatvédelem fogalmainak technológiasemleges definíciói elvileg szilárd alapokat jelentenek. A fogalmi rendszer elemei közül a személyes adat definíciójának értéke az, hogy az adatok széles körét foglalja magában; ugyanakkor azt is látni kell, hogy lehetőséget ad olyan kiterjesztő, tág értelmezésre is, ami azzal jár, hogy digitális környezetben – figyelembe véve a tudományos-technikai fejlődést – előbb-utóbb bármilyen információ a természetes személy azonosíthatóságát fogja eredményezni (pl. VIN-szám). Ennek ellenére nem tudok egyetérteni a digitális omnibusz csomag javaslatának azzal a pontjával, amely szubjektív mércéhez köti az azonosíthatóság kritériumát, így próbálja szűkíteni a személyes adatok körét. Félő, hogy a mozgó, mobil értelmezésű fogalom az érintettre vonatkozóan hátrányt, különböző védelmi szintet okoz majd. Szintén problémaként értékelem azt, hogy az információk értelmezését bizonytalanságot okozó elemek nehezítik, ezt példázza az érintettet azonosító fénykép, amely mint személyes adat és mint különleges személyes adat is szóba jöhet, attól függően, hogy biometrikus azonosításra alkalmas technológiával kezelték-e, vagy sem. Az érintett védelme szempontjából kiemelkedő jelentőségű a személyes adat vagy anonimizált adat kérdése. A gyakorlat azt mutatja, hogy az anonimizálás nem hatékony módszer, az újraazonosításnak valós kockázata van. Az oka lehet módszertani probléma, amire megoldást jelenthet a módszertani kérdések ágazati, esetleg intézményi kidolgozása; de akár rendszerszintű problémára is utalhat. Októl függetlenül mindenképpen alááshatja az érintettek védelmét.

Az érintettek személyes adatainak védelme tekintetében a jogszabálytípus, a területi hatály és a fogalmi apparátus alapvető horderejük, de önmagukban nem elegendők, szükséges maguknak az érintetteknek is jogokat biztosítani. Az adatkezelés folyamatára kontrollt biztosító érintetti jogok közül kettőt tudok kiemelni, amelyek nemcsak elméletben, de a gyakorlatban is intenzív védelmet biztosítanak. Az egyik a tiltakozáshoz való jog, amely ún. abszolút jog, és a közvetlen üzletszerzési célú hirdetések ellen is hatásos eszköz. A másik nem jogként

fogalmazódik meg, mégis a legerősebb védelmet biztosítja az adatkezelésre vonatkozó általános tilalommal az olyan, kizárólag automatizált adatkezelésen és profilalkotáson alapuló döntés hatálya ellen, amely az érintettre nézve joghatással bír, vagy őt jelentős mértékben érinti. Ezt a nagyon értékes védelmi funkciót kívánja lerontani a digitális omnibusz csomag javaslata azzal, hogy szerződéskötéshez és -teljesítéshez lehetővé teszi az algoritmikus döntéshozatalt még akkor is, ha a döntés nem kizárólag automatizált módon hozható meg. Vannak továbbá olyan érintetti jogok, amelyek elméletileg erős védelmet biztosítanak az adatalanyok számára, a gyakorlatban azonban kevésbé működőképesek (a helyesbítéshez való jog a kikövetkeztetett adatok és a profilalkotás tekintetében, az adathordozhatósághoz való jog az interoperabilitás kötelező előírásának hiánya miatt, az elfeledtetéshez való jog a több adatkezelőhöz továbbított adatok esetében nehezen érvényesíthető).

Az érintettek védelmét szolgálja az is, hogy az adatkezelő felelősségére építve preventív és mindent átható szabályokat fogalmaz meg a jogalkotó, ezek az ún. adatkezelési alapelvek. A célhoz kötöttség, az adattakarékosság, a korlátozott tárolhatóság, a tisztesség, mind-mind hatékony elvek, éppúgy, mint a GDPR lehangsúlyosabb újdonsága, a beépített és alapértelmezett adatvédelem, valamint az adatvédelmi hatásvizsgálat. Ha az adatkezelő nem csak formai kötelezettségként tekint az adatvédelmi hatásvizsgálatra, akkor vezérfonalat nyújt az egyedi sajátosságok és a GDPR-rendelkezések összhangba hozására és a fenyegető kockázatok minimálisra csökkentésére. Úgy vélem, hogy az adatvédelmi hatásvizsgálat nemcsak az érintetti adatok védelmét támogató értékes eszköz, ami egyúttal képes előkészíteni a tisztességes döntési környezetet biztosító alapértelmezett beállítások lehetőségét is, hanem a szolgáltatók önszabályozási eszközévé is válhat egyben.

Ellenőrzésre a tagállami felügyeleti hatóságok jogosultak, de a GDPR a határokon átnyúló ügyek tekintetében egyablakos ügyintézési eljárást ír elő. Ez kétségtelen előnyöket hordoz a vizsgálat alá vont vállalatok számára, de súlyos végrehajtási problémákat okoz, mert alig néhány fő felügyeleti hatóságnál koncentrálódnak a nagy ügyek, s csak az együttműködési eszközök kimerítése után kerülhet sor az egységességi mechanizmus keretében való kezelésre, ami a folyamat végén az EDPB bekapcsolódását jelenti. A nagy ügyek esetében a végrehajtás aránytalan, lassú és nem hatékony. További problémát okoz az, hogy fő felügyelő hatósági szerepet éppen annak a tagállamnak a hatósága kap, ahol a platform tevékenységi központja van, s ahol, e tényből következően, jelentősek a tagállam platformokhoz kapcsolódó gazdasági érdekei is. Már hatályos, de még nem alkalmazandó a GDPR eljárási rendelete, amely – véleményem szerint – az alapproblémát nem fogja orvosolni; valódi megoldást a nagy ügyek tekintetében a végrehajtás központosítása jelentene, mint a DMA vagy a DSA esetében. Mivel

a DMA rendelkezéseinek megsértése esetén centralizált a végrehajtás, ez közvetve hozzájárulhat az adatvédelmi hatóságok leterhelésének csökkenéséhez, de a kapuőrré válás előtt álló vállalkozások okozhatnak újabb, adatkezeléssel összefüggő meglepetéseket, ezzel együtt újratermelve a végrehajtási kérdéseket is. Szintén rendszerszintű végrehajtási problémát hozott felszínre a Facebook kontra Bundeskartellamt ügy. Az EUB-ítélet szerint, ha a gazdasági szereplő visszaélészerű magatartásának megállapításához az adatvédelmi szempontok vizsgálata szükséges, akkor ezt a tagállami versenyhatóság megteheti, és megállapíthatja a jogsértést a GDPR vonatkozásában. Az EUSZ nem tartalmazza a benne foglalt lojális együttműködés elve konkrét kereteit és szabályait, ezt pótolta az EU esetjoga, és erősítette meg az EDPB, ami más hatóságok közötti együttműködésre is irányadó lehet.

A felhasználók számára a hírközlő hálózatokon továbbított közlések és az eszközein tárolt adatok tekintetében is védelmet kell biztosítani, ezt jelenleg az elektronikus hírközlési adatvédelmi irányelv szabályozza. A GDPR-t kell azonban alkalmazni minden olyan esetben, amelyekre nem vonatkoznak az irányelvben meghatározott különös kötelezettségek, jellemzően a végfelhasználó eszközén elhelyezett cookie-k tartoznak ide. Egy részük elengedhetetlen a honlapok működéséhez, más részük a felhasználók személyes jellemzőinek, helyzetének, preferenciáinak megállapításához visz közelebb. A jelenlegi irányelv nem védi megfelelő szinten a felhasználókat, nem védi őket a közvetlen üzletszerzési célú üzenetektől, rendelkezései nem kezelik a technológiai kihívásokat, és a tagállami implementáció akadályozza az egységes alkalmazást. E problémákat a jogalkotó előbb az e-Privacy rendeletre, jelenleg pedig a digitális omnibusz csomagra irányuló jogalkotási eljárással kívánja megoldani. A versenyképesség növelését célzó csomag javaslata szerint az elektronikus hírközlési adatvédelmi irányelv szabályozási köréből a cookie-kra vonatkozó szabályok a GDPR hatálya alá kerülnek, összekapcsolva ezzel a végberendezéshez való hozzáférést és az adatkezelést, a beleegyezés-fáradtság kezelésére beépített megoldást javasol. A cookie-falakat azonban nem szabályozza, és szubjektív mércéjű döntést irányoz elő a személyes adatokkal kapcsolatban. E változat elfogadása összességében tehát csökkentheti az adatvédelem szintjét.

A fentiek igazolják hipotézisemet. *Korunk érintettjeinek egységes védelméhez stabil vázat biztosít a GDPR rendeletjellege, területi hatálya, kockázatkezelése és az alapelvek rendszere. Technológiasemleges fogalomrendszere rugalmas, de a digitális környezet és a technológiai kontextus egyre inkább feszegeti adekvátságát. Végrehajtását a decentralizált struktúra nehezíti, s ezen a GDPR eljárási rendelete csak korlátozottan fog tudni segíteni. Az érintetti jogok tartalma erős kontrollt biztosít, de a gyakorlatban felvet alkalmazhatósági problémákat. Az elektronikus hírközlési adatvédelmi irányelv, a cookie-kra vonatkozó*

szabályozás terén, nem biztosít egységes védelmet a felhasználók számára, főleg az eltérő tagállami implementációból következően.

3. A személyes adatok kezelése és a piaci verseny összefüggése alapján a GDPR mely rendelkezései váltak további szigorítást motiváló tényezővé, valamint a platformjogszabályokban testet öltő szigorítások milyen irányban képesek befolyásolni a piaci versenyt?

Az erőfölénnyel való visszaélést vizsgáló és a fúziós ügyek tapasztalatai egyaránt rámutattak arra, hogy a digitális gazdaságban a személyes adatok kezelése és a piaci verseny alakulása között szoros kapcsolat van. A hatalmas adatvagyon nyersanyagot jelent a platformok számára, amely lehetővé teszi a felhasználói viselkedés elemzését, a felhasználók célzását reklámokkal, kapcsolatépítést az üzleti felhasználókkal stb. A személyes adatok nem mindig tisztességes megszerzése, szolgáltatásaik közötti összekapcsolása nemcsak piaci erőfölényhez, hanem az ezzel való visszaéléshez is vezethet, belépési korlátot képezve a többi piaci szereplő számára. Az adatvagyon nagyságát, egyszersmind a piacra gyakorolt hatást a fúziók tovább növelhetik. Ennek ellenére a Bizottság a 2010-es évek közepéig kitartott amellett, hogy a magánélet és a személyes adatok védelme nem tartozik a versenyjogi értékelés szempontjai közé, és fordulat csak akkor következett be, amikor a Facebook a saját és a felvásárolt WhatsApp-adatbázist egyesítette.

A nagy online platformok tisztességes adatkezelési és piaci magatartásra ösztönzése, egyszersmind a kisebb vállalkozások segítése, a piacok megmozgatása érdekében a jogalkotónak meg kellett acélosítania a GDPR rendelkezéseit. E célok elérésére legalkalmasabb a GDPR jogalapokkal kapcsolatos és adathozzáféréssel, -hordozhatósággal kapcsolatos rendelkezéseinek megerősítése és kiegészítése volt a DMA-ben, amelyek által egyúttal tiszteletben tartható az EUMSZ 102. cikkének elvárása: az erőfölény ellen nem lép fel, de az ezzel visszaélő piaci magatartást regulázza.

Míg a GDPR a jogalapok tekintetében széles lehetőséget hagyott az adatkezelők számára, addig a DMA letette a voksot a mérlegelési lehetőséget sem engedő szabályozás mellett, oly módon, hogy differenciáltan és célzottan csak a kapuőröket regulázza. A DMA értelmében a kapuőr csak hozzájárulás alapján kezelheti és kapcsolhatja össze a személyes adatokat, de nem használhatja fel azokat a nyilvánosan nem elérhető adatokat, amelyek az üzleti felhasználók tevékenységével összefüggésben keletkeznek, vagy amelyeket üzleti felhasználók vagy azok ügyfelei adtak meg vagy generáltak. A DMA több tekintetben kiterjesztette a GDPR-

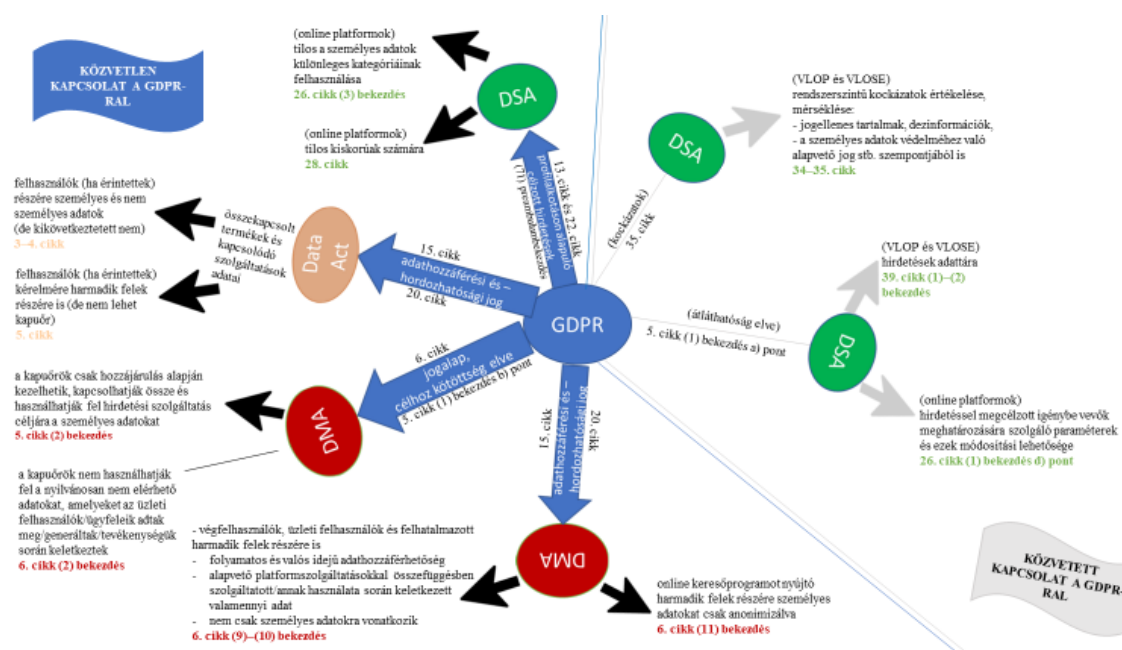
ban foglalt adathozzáférési és -hordozhatósági jogot is – a végfelhasználók, a jogi személy üzleti felhasználók és felhatalmazott harmadik felek részére is folyamatos és valós idejű adathozzáférhetőséget biztosít az alapvető platformszolgáltatásokkal összefüggésben szolgáltatott vagy annak használata során keletkezett valamennyi adatra vonatkozóan –, ezáltal lehetővé téve a fogyasztók szolgáltatóváltását, valamint az adatoknak a gazdaságba való erőteljesebb beépülését. Szintén ez utóbbi célt szolgálja az a rendelkezés, hogy az online keresőprogramot nyújtó harmadik felek részére a kapuőrnek hozzáférést kell biztosítania a keresőprogramjával végzett végfelhasználói keresések során generált adatokhoz.

A GDPR adathozzáférési és -hordozhatósági jogának továbbgondolásából egy teljes rendelet is született, a Data Act, amely a 2026 szeptemberétől forgalomba kerülő IoT-termékek esetében a gyártót kötelezi arra, hogy a szolgáltatás nyújtása során visszanyert vagy generált adatok alapértelmezés szerinti, közvetlen hozzáférhetőségét biztosítsa a felhasználó számára; ez idő előtt az adatbirtokosnak kell gondoskodni a hozzáférhetővé tételről. Az IoT-termékek felhasználói nemcsak hozzáférhetnek, de használhatják és meg is oszthatják a generált adatokat, ideértve a személyes és a nem személyes adatokat is, és felhasználói kérésre e jogokat harmadik felek részére is biztosítani kell. Bár a GDPR biztosítja az érintettek számára az adathordozhatósági jogot – úgy gondolom –, a gyártók Data Actben foglalt kötelezésétől várható nagyobb léptékű elmozdulás, ami előhívhatja a felhasználók, a fogyasztók aktivitását, egyúttal az adatok gazdaságba csatornázását vonva magával.

Értékelve a platformjogszabályokat, közülük a Data Act korát meghaladó szemlélettel támogatja az adatmegosztást, amely ezáltal elősegíti az adatoknak a gazdaságban való forgását, ezzel együtt az európai adatgazdaság erősödését és versenyképessé válását. E képességei miatt a digitális omnibusz csomag javaslata alapján a Data Act lesz az uniós adatgazdaság egyik központi rendelete. Valódi értékét majd az fogja megmutatni, hogy a felhasználók, a fogyasztók mennyire lesznek képesek élni a lehetőségekkel, ill. hogy a kedvezményezettek mennyire tudják kiaknázni a rendeletben rejlő potenciált. A Data Acthez viszonyítva a DMA, véleményem szerint, megkésett rendelet, de előnye az, hogy ex ante lép fel, és a címzettek körének változását is lehetővé teszi. Ezzel egyenlőbb versenyfeltételeket és tisztességesebb üzleti környezetet teremthet, és felerősítheti az innovatív erőforrásokat. A DMA-t azért tartom megkésettnek, mert a beleegyezés-fáradtság miatt az adatvédelmi problémák megoldásához jelentős mértékben már nem tud hozzájárulni. Ezen túlmenően a DMA a piaci versenyt úgy kívánja támogatni, hogy egyúttal engedi újratermelni az adatvédelmi problémákat, ami arra enged következtetni, hogy az EU nem védi akaratauk ellenére a felhasználókat, fogyasztókat, de megteremti számukra a lehetőséget adataik védelmére.

Hipotézisemet igazolta elemzésem. A vizsgált versenyügyek rámutattak arra, hogy a platformok személyesadat-kezelése és a piaci verseny alakulása között szoros a kapcsolat, a nagy adatvagyonoknak meghatározó szerepük van a piaci versenyben és az erőfölénnyel visszaélő magatartásban. A GDPR azon rendelkezéseit kellett megerősíteni a platformjogszabályokban, amelyek a platformok tisztességtelen adatkezelése által hozzájárultak a nagy adatvagyonok létrejöttéhez és felhasználásához saját üzleti célra, ezzel együtt a platformok versenykorlátozó magatartásához. A GDPR-ból a hozzájárulás kapott sokkal karakteresebb szerepet a DMA-ben, valamint az érintetti jogok közül az adathozzáférési és -hordozhatósági jog szintén a DMA-ben és a Data Actben. A platformok adatkezelésének korlátozása és a személyes adatok mobilizálhatósága elősegítheti a piaci versenyt. A GDPR és a platformjogszabályok kapcsolatát mutatja az 1. ábra.

1. ábra: A GDPR és a platformjogszabályok kapcsolata



Forrás: saját szerkesztés az ábrán feltüntetett jogszabályok alapján

4. Az EU fogyasztóvédelmi eszközrendszere képes-e a fogyasztók – személyes adatokkal kapcsolatos – aszimmetrikus helyzetének kezelésére?

Az uniós fogyasztóvédelmi jog – a digitális környezet és a platformok súlyának növekedése miatt – úgy igyekszik megerősíteni a fogyasztók védelmét az adataik kezelése tekintetében, hogy a klasszikus szabályozási területek rendelkezéseit egészíti ki.

A fogyasztóvédelmi tárgyú uniós jogszabályok többsége, ahol ez releváns, a fogyasztó tájékoztatásával, az átláthatóság előírásával kívánja az információs aszimmetriát ellensúlyozni. A távollévők között kötött és az üzlethelyiségen kívül kötött szerződéseket a CR-irányelv szabályozza, és azzal védi a fogyasztókat, hogy számukra többlettájékoztatást kell nyújtani, többek között arról, hogy az ár személyre szabott-e. Több, a hirdetések azonosíthatóságát biztosító átláthatósági intézkedést fogalmaz meg a DSA, amelyek a kéréstlen hirdetések kontrollálását szolgálják, továbbá az online óriásplatformot és a nagyon népszerű online keresőprogramot üzemeltető szolgáltatóknak a hirdetési adattárakat is nyilvánosan hozzáférhetővé kell tenniük.

A fogyasztóvédelmi eszközrendszer másik elemét a szerződések szabályozása jelenti. A CR-irányelvtől kézzelfoghatóbb – a szerződésszerű teljesítésre, a jogorvoslati lehetőségekre stb. vonatkozó – jogokat biztosít a fogyasztók részére a DCS-irányelv. Elismeri a digitális tartalom vagy szolgáltatás pénzbeli ellentételezés nélküli nyújtását, bár az ilyen típusú szerződés fogalmát nem definiálja, és a szolgáltatás devalválása ellen sem véd. A UCT-irányelv az egyedileg meg nem tárgyalta szerződések esetén védi a fogyasztókat a tisztességtelen feltételektől, de melléklete sem a digitális piacokkal, sem a platformokkal kapcsolatban nem tartalmaz tisztességtelen feltételt, pedig jogesetek tanúsága szerint az online platformok éppen az általános szerződési feltételek mögé bújva gyűjtik tisztességtelenül a személyes adatokat.

A kockázatok értékelése és mérséklése alkalmas arra, hogy védje a fogyasztói, felhasználói érdeket. A GDPR és a DSA is fókuszba állítja a kockázatkezelést és -csökkentést, de míg az előbbi a magas kockázattal járó adatkezelési műveletek tekintetében az adatkezelő által meghatározott szempontú adatvédelmi hatásvizsgálatot ír elő, utóbbi a rendszerszintű kockázatok meghatározott kategóriára vonatkozó kockázatértékelési kötelezettséget telepít, de csak az online óriásplatformokra és a nagyon népszerű online keresőprogramot üzemeltető szolgáltatókra. Ez utóbbiak várhatóan a fogyasztók erősebb védelmét fogják biztosítani, különösen úgy, hogy évente független ellenőrzésnek is kapcsolódni kell hozzá.

A gyermekeket mint kiszolgáltatott fogyasztói csoportot erőteljesen védi a jogalkotó. A UCP-irányelv – bár az őket célzó reklámokat nem tiltja – agresszív kereskedelmi gyakorlatnak minősíti a gyermekek felszólítását vásárlásra. A GDPR rendelkezései alapján profilozás nem végezhető (legfeljebb a jólétük érdekében, jogszabályi kivételek alapján), ebből következően a célzott reklámozás sem megengedett. A DSA egyértelmű tilalmat állapít meg a kiskorúak személyes adatait felhasználó, profilalkotáson alapuló hirdetések tekintetében, amely azonban csak az online platformokra vonatkozik. E differenciált tilalom annak lenyomata, hogy a jogalkotó számára erősebb motivációt jelentett a platformok regulációja, mint a gyerekek

érdeke. Véleményem szerint szükséges a tilalom egységes kiterjesztése minden olyan szolgáltatóra, amely információt terjeszt, ugyanígy a személyes adatok különleges kategóriáit felhasználó, profilalkotáson alapuló célzott reklámozást is egységesen tiltani kellene.

A UCP-irányelv rendelkezései és melléklete, hasonlóan a UCT-irányelvhez, nem nevesít kifejezetten a személyes adatokkal összefüggésbe hozható, különösen a sötét megoldásokkal kapcsolatos tiltott kereskedelmi gyakorlatokat – s bár a Bizottság iránymutatása szerint ezek kezelhetők a rendelkezések és a meglévő feketelista alapján –, hiányuk jelentősen nehezíti az ilyen ügyekben indult eljárásokat. A fogyasztóvédelmi eszközrendszer további széttöredezettségéhez vezet az, hogy az egyre szaporodó sötétmegoldás-típusok szabályozási válaszreakciót váltottak ki több jogszabályban is. A sötét megoldások kezelésében a UCP-irányelvre terhelődik a legerőteljesebb szerep, ugyanis ha valamely magatartás nem tartozik a DMA vagy a DSA hatálya alá, akkor megoldást csak az jelenthet, hogy be kell illeszteni a tisztességtelen kereskedelmi gyakorlatok közé. Ez a tény tovább súlyosbítja a személyes adatokkal kapcsolatos tiltott magatartások feketelistájának hiányát a UCP-irányelvben. Ezen túlmenően nemcsak további széttöredezettséget, hanem koherenciaproblémákat is felvet, ami az egységes fogyasztói védelem ellen ható tényező. A széttöredezettség és a koherenciaproblémák nem csupán a sötét megoldások terén jelentkeznek, hanem a profilalkotás és a személyre szabott hirdetések szabályozása során is jelentősek.

A profilalkotás, az algoritmusok és más átláthatatlan technológiák miatt a digitális térben folyamatosan erősödik az aszimmetria, ebből következően az átlagfogyasztó is kiszolgáltatottá, sérülékennyé válhat; az átlagfogyasztó fogalom mégsem tartalmaz erre vonatkozó elemet. Megoldásként szóba jöhet a UCP-irányelv módosítása, de a jogi normák rendszerszerű technikai beágyazása is, amely a szolgáltatókra terhelné a szabályozási adminisztrációt, elismerve egyúttal szabályozói képességüket is. A digitális sérülékenységet az EU a digitális méltányossági törvénnyel, a DFA-vel kívánja kezelni, jelenleg a jogalkotási folyamat előkészítése zajlik.

A fogyasztóvédelmi eszköztár elemeire rétegzett adatvédelmi rendelkezések nagymértékű és egyre gyakoribb megjelenése miatt vetődött fel annak lehetősége, hogy sajátos szabályozási terület van kialakulóban, amit fogyasztóvédelmi adatjognak neveztem. Azonban a jogszabályi védelem jellegének különbözősége, valamint az önálló intézmény- és a fogalomrendszer hiánya, de leginkább az elkülönült jogalanyiség hiánya alapján azt kell megállapítani, hogy nem beszélhetünk önállósuló fogyasztóvédelmi adatjogról; sőt ezt erősítik a koherenciahiány fentebb említett esetei is. Mindezekből következően cáfolni kell hipotézisemnek ezt a részét.

A GDPR-ra összpontosító fejezetben a fogyasztóvédelmi kitekintések, valamint a fogyasztóvédelem eszközrendszerét a személyes adatok tekintetében vizsgáló fejezet megállapításai elvezettek abba az irányba, hogy a GDPR, valamint a DSA és a klasszikus fogyasztóvédelmi jog között több ponton (területi hatály, ex ante szabályozás, gyermekek védelme stb.) kimutatható párhuzam érvényesül, amelynek középpontjában a fogyasztó, a fogyasztó védelme áll. A fejlődési folyamat kidomborítja azokat az értékeket, amelyek évtizedek óta irányítják a fogyasztók védelmét az EU-ban. (A teljes szempontsört és a folyamatot a 6. melléklet mutatja.)

A 4. kérdésre vonatkozó megállapításaim a várakozásomnak megfelelők: *Digitális környezetben a fogyasztóvédelem és az adatvédelem gyakran metszi egymást, ezért a jogalkotó a gyengébb fél védelmét a klasszikus fogyasztóvédelmi eszközökre rétegzett adatvédelmi rendelkezésekkel erősíti meg. Ez hozzájárul a fogyasztók aszimmetrikus helyzetének mérsékléséhez, teljes mértékben azonban nem képes azt felszámolni. Ennek egyik oka az, hogy a digitális térben az átlagfogyasztó is sérülékennyé válhat, de a digitális sérülékenységek kezelésére vonatkozóan még csak körvonalazódnak a jogalkotás szálai. Elengedhetetlenül szükséges lenne tehát a fogyasztóvédelmi jognak gyorsabban és következetesebben reagálnia a digitális környezetre. Másik oka az, hogy mivel a fogyasztóvédelmi jog horizontálisan kapcsolódik más jogterületekhez, ezért más a megközelítés és a szabályozás logikája is, ami különösen az adatvédelemmel összefüggő fogyasztóvédelmi szabályozásban növeli a széttöröttségét és a koherenciaproblémákat. A jéghegy csúcsait a sötét megoldások, a profilalkotás és a személyre szabott reklámok jelentik.*

Hipotézisem második felét cáfolnom kell: a fogyasztóvédelmi jognak a személyes adatok kezelésével összefüggő rendelkezései nem alapozzák meg a fogyasztóvédelmi adatjog kialakulását; a védelem jellege, a jogalanyok, valamint az intézmény- és fogalmi rendszer vizsgálata nem támasztja ezt alá. Ugyanakkor a fogyasztóvédelemnek van egy egyre erősödő adatvédelmi szegmense.

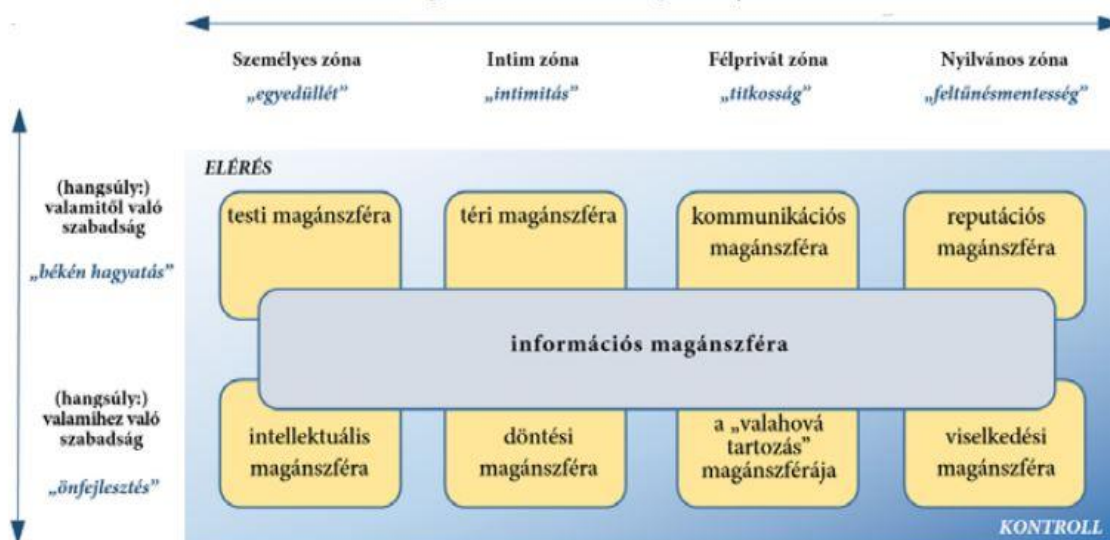
Disszertációm a személyes adatok kezelésének teljes körképét fogta át, ezáltal elvezetett digitális környezetben az adatvédelem, a versenyjog és a fogyasztóvédelem metszéspontjainak feltárásához, a piaci versenyre és a fogyasztókra gyakorolt hatás értelmezéséhez. Fogyasztóvédelmi adatjogról nem beszélhetünk, az azonban leszögezhető, hogy a digitális környezetre vonatkozóan erősödőben van a fogyasztóvédelmi jogszabályokban az adatvédelmi rendelkezések megjelenése, megszilárdítva a fogyasztók jogait az adatvédelem területén is. Ez a folyamat jelenleg ott tart, hogy ezek kölcsönösen erősítik egymást: a fogyasztóvédelem

nézőpontja érvényesül az adatvédelemben, az adatvédelem szemlélete pedig beépül a fogyasztóvédelembe.

A folyamatban lévő uniós jogalkotási folyamatokkal kapcsolatban azt az álláspontot képviselem, hogy kívánatos lenne, ha a készülő DFA rendelet lenne, ezáltal horizontális szinten lenne képes a digitális sérülékenységet kezelni, és illeszkedne az EU digitális szabálykönyvének rendszerébe is. A digitális omnibusz csomag javaslatának nem minden pontjával értek egyet, ezért úgy vélem, egyértelmű határokat kellene megállapítani az adatvédelmi célok és az adatok gazdasági hasznosítása céljai tekintetében.

MELLÉKLETEK

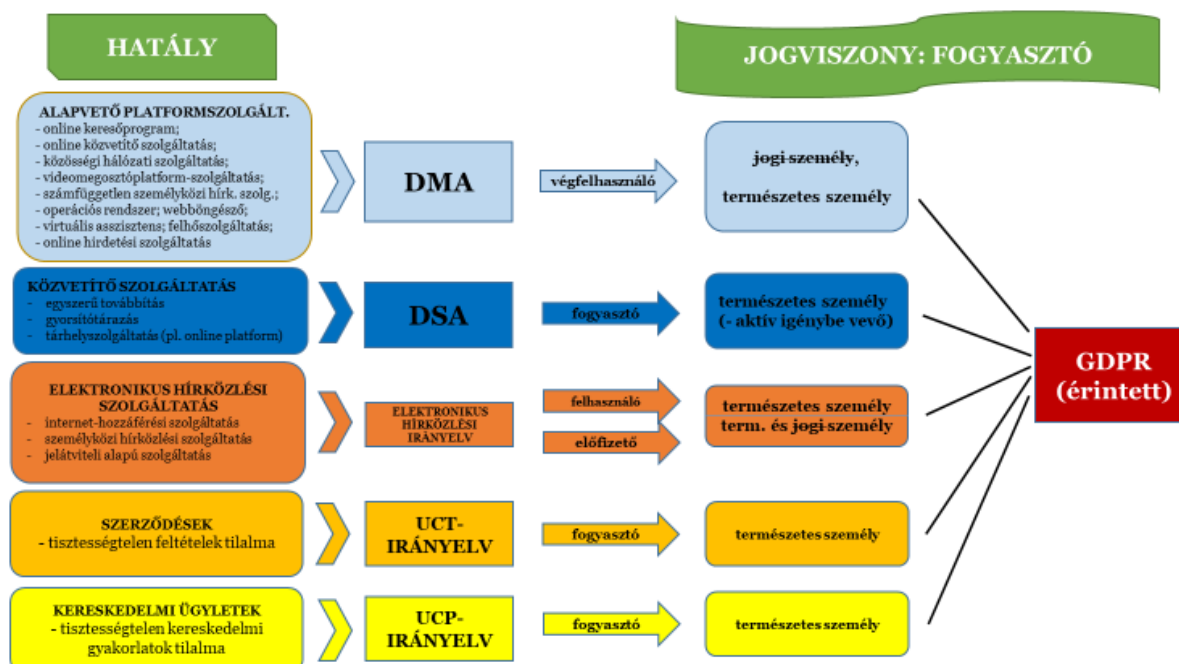
1. melléklet: A magánélet tipológiája



Forrás: KOOPS–NEWELL–TIMAN–ŠKORVÁNEK–CHOKREVSKI–GALIČ i. m. 566.

Magyar fordításban közli a NAIH STAR-projekt: 1. témakör – Bevezetés az uniós adatvédelmi rendszerbe 12. dia. <https://www.naih.hu/star-i/stari-eredmenyek> (letöltés: 2023. 02. 02.)

2. melléklet: Érintett és fogyasztó – az online szolgáltatásokkal összefüggésben



Forrás: saját szerkesztés az ábrán feltüntetett jogszabályok alapján

3. melléklet: A profilalkotás intézménye és a kockázatok a különböző szektorokban

Szektor, ágazat	Jogalany	Profilalkotás / automatizált döntés példaterületei	Joghatás vagy jelentős mértékű hatás	Kockázatok az érintettek vonatkozásán
Foglalkoztatás	álláskereső, munkavállaló	álláspályázatok szűrése, teljesítmény-értékelés	megélhetést érintő joghatás	diszkrimináció
Oktatás	tanuló, hallgató	felvételi rangsor, lemorzsolódási profil	továbbhaladásra hat	beskatulyázás
Egészségügy	biztosított, ellátott, beteg	betegségkockázati profil, ellátási sorrend, kezelési javaslat	egészséghez, élethez való jog	hibás döntések, visszafordíthatatlan károsodás
Szociális ellátások	állampolgár, ellátott	jogosultság megállapítása, támogatási rangsor	alapjogokat érint (szociális biztonság)	kiszolgáltatottság, kirekesztettség
Pénzügyi szektor (biztosítás, hitel)	ügyfél, fogyasztó	hitelképesség vizsgálata, díjtétel, futamidő, hitelkeret, kamat	gazdasági joghatás (hitelhez, biztosításhoz jutás)	pénzügyi hátrány, hozzáférési hátrány, profilcsapda
Kereskedelem (nem reklám)	felhasználó, fogyasztó	profilról függő személyre szabott ár, terméksorrend	gazdasági hátrány	túlárazás, döntés manipulálása

Forrás: saját szerkesztés a GDPR 22. cikk (1) bekezdés figyelembevételével

4. melléklet: Az adatvédelmi hatásvizsgálat folyamatának lépései



Forrás: WP248. 8.

5. melléklet: A digitális piacon érintettek helyzete a DMA alkalmazása előtt és után

Érin- tettek	Helyzetük a DMA előtt	Helyzetük a DMA által
Végfelhasználók (= fogyasztók)	ingyenes platformhasználat → személyes adatokkal „fizetés”	
	közvetlen hálózati hatást indukálnak	
	adathordozhatóság (GDPR 20. cikk)	tényleges adathordozhatósági jog folyamatos és valós idejű hozzáféréssel, mely vonatkozik a végfelhasználók által felhatalmazott harmadik felekre is (kiegészíti a GDPR 20. cikkét) <i>DMA 6. cikk (9) bekezdés</i> ↓ lehetővé teszi a platformok, szolgáltatások közötti váltást vagy a párhuzamos használatot
	személyes adataik felhasználása és kombinálása az érintett platform alapszolgáltatásán kívül (profilalkotás által)	személyes adataik kapuőr általi keresztfelhasználásának, összekapcsolásának (≡ GDPR célhoz kötöttség) engedélyezéséről dönthetnek (GDPR 7. cikk, de egyedüli jogalap a hozzájárulás), mely vonatkozik a kapuőr által nyújtott más szolgáltatásból és a harmadik fél által nyújtott szolgáltatásból származó adatokra is <i>DMA 5. cikk (2) bekezdés</i> ↓ a szolgáltatás hozzájárulás nélkül is elérhető
	az előre telepített szoftvereket és alkalmazásokat használhatták (vevőfogvatartás)	nem függenek a kapuőrök alapértelmezett beállításaitól <i>DMA 6. cikk (3) bekezdés</i> ↓ választhatnak más szolgáltatásokat, alkalmazás-áruházakat, alapértelmezett beállításokat stb., nem csak a kapuőrökét
	az üzleti felhasználók szolgáltatásaihoz csak a kapuőrökön keresztül tudtak eljutni	az üzleti felhasználó szoftveralkalmazásán keresztül – de a kapuőr platformszolgáltatásai révén – hozzáférnek tartalmakhoz, előfizetésekhez stb., és használni is tudják ezeket <i>DMA 5. cikk (5) bekezdés</i> ↓ a platformszolgáltatás beállításaitól függetlenül, szabadon választhatják és kapcsolhatják össze a szolgáltatásokat stb.
	rangsorolással befolyásolás: a kínált	a platform nem részesítheti kedvezőbb elbánásban az általa kínált hasonló

nagyobb választék és az innováció okozta előnyök

	hasonló termékek/szolgáltatások közül a sajátjait helyezi előre a keresési eredményekben (önpreferencia)		termékeket/szolgáltatásokat harmadik felekéhez képest DMA 6. cikk (5) bekezdés ↓ releváns keresési eredmények	
Üzleti felhasználók	közvetett hálózati hatás			
	adathordozásra nincs lehetőség	függőség; tisztességtelen, kizsákmányoló üzleti környezet	- a végfelhasználó által felhatalmazott harmadik felek számára: tényleges adathozzáférési és adathordozhatósági jog folyamatos és valós idejű hozzáféréssel DMA 6. cikk (9) bekezdés - interoperabilitási célú hozzáférés biztosítása (hardver-, szoftverfunkciók) DMA 6. cikk (7) bekezdés	egyenlő versenyfeltételek, tisztességesebb üzleti környezet
	korlátozás az értékesítési csatornákra vonatkozó szerződéses feltételekkel		- szolgáltatásaikat, termékeiket, alkalmazásaikat más csatornákon is értékesíthetik - szerződéseket köthetnek ügyfeleikkel, hirdethetik termékeiket a kapuór platformján kívül is DMA 5. cikk (3)–(4) bekezdés	
	az üzleti tevékenységük által keletkezett, nyilvánosan nem elérhető adataik (végfelhasználóiktól származók is) felhasználása az érintett platform által saját célra		üzleti tevékenységük által keletkezett, nyilvánosan nem elérhető adataikat az érintett platform nem használhatja saját célra (végfelhasználóiktól származókat sem) DMA 6. cikk (2) bekezdés	
az adat = nyersanyag, input				
Online platformok	big data → szolgáltatnak a piac mindkét oldalának			
	új terméket nem hoznak létre, hanem technikailag összekapcsolják a kínálati és a fogyasztói igényeket			
	a hálózati hatások nyertesei	várhatóan osztoznak a versenytársakkal a hálózati hatásokon		
	extrém megtérülési ráta → tőkefelhalmozás	a verseny alapján részesülnek a profitból		
	monopolhelyzetet, túlhatalom → függőségek	várhatóan megszűnik a monopolhelyzetük és ennek következményei		
	melléjük új vállalkozásoknak szinte lehetetlen a piacra lépni	új vállalkozások is piacra léphetnek		
	piaci erőfölényt szerezhetnek, ezzel visszaélhetnek	nehezebb erőfölényt szerezniük és azzal visszaélni, mert a belépő vállalkozások versenytársakká válhatnak		

Versenyjogi kezelése	EUMSZ 102. cikkében foglalt erőfölénnyel visszaélés (hosszú és eseti alapú eljárás, bizonytalan végkimenetel, nem visszatartó erejű bírság)	DMA 5. és 6. cikk
	= utólagos szabályozás	= előzetes (ex ante) szabályozás = megelőzni kívánja a visszaéléseket (de a rendelkezések megsértése esetén: EUMSZ 102. cikk)

Forrás: saját szerkesztés az EUMSZ 102. cikke, a DMA preambuluma, valamint az 5. és 6. cikke; TÓTH–SZABÓ–NÉMETH–RUDICS–RIDEĞ *i. m.* 45–68.; ZÓDI Zsolt (2022) *i. m.* 68. alapján

6. melléklet: A fogyasztóközpontú uniós szabályozási logika területei és fejlődése

Vizsgált szempont	Klasszikus uniós fogyasztóvédelem	GDPR	DSA	A fogyasztói fókusz közös vonása
Jogalany	fogyasztó	érintett	felhasználó	kiszolgáltatót fél
Területi hatály	a tevékenység a fogyasztó tagállamára irányul (Brüsszel Ia., Róma I.)	az érintettek megcélzása, viselkedésük megfigyelése az EU-ban	uniós felhasználók részére nyújtott szolgáltatás, független a szolgáltató letelepedési helyétől	a letelepedési elv helyett a fogyasztó/felhasználó helyzete a döntő
Gyengébb fél védelme	a fogyasztók védelme a piaci egyensúly érdekében	érintetti autonómia biztosításával	a felhasználók védelme a manipulációtól	az aszimmetriát rendszerszinten kezeli
Információs aszimmetria kezelése	előzetes tájékoztatási kötelezettségek (CR-irányelv, UCP-irányelv)	átláthatóság, hozzáférési jog, adatkezelési tájékoztató	átláthatóság növelése, pl. hirdetések átláthatósága	a döntési autonómiát információkkal támogatja
Egyéni kontroll	elállási jog (CR-irányelv), hibás teljesítés orvoslása (DCS-irányelv)	helyesbítés, törlés, adatkezelés korlátozása stb.	felhasználói döntések tudatosabbá tétele, pl. nem profilalapú hirdetések választása	aktív fogyasztói/érintetti magatartás
Gyermekek védelme	különösen kiszolgáltatót fogyasztó védelme (UCP-irányelv)	közérthető tájékoztatás, hozzájárulás érvényessége: 13–16 év	profilalkotás alapú célzott reklám tilalma, jogait érintő kockázatok értékelése	gyermekek sebezhetősége ↓ erősebb védelem
Ex ante eszközök	tisztességtelen kereskedelmi gyakorlatok tilalma (UCP-irányelv)	beépített és alapértelmezett adatvédelem	sötét megoldások tilalma, tisztességes interfész kialakítás	jogsértések megelőzése > utólagos szankció
Végrehajtás	hatósági együttműködésen alapul	egyablakos mechanizmus; GDPR eljárási rendelete; panaszbefogadhatósági harmonizáció	központosított végrehajtás	a végrehajtás fokozatos erősödése és központosítása

Forrásai: saját szerkesztés a táblázatban felsorolt jogszabályok alapján, de motiválón hatottak a vizsgálódás irányának kijelölésében: HELBERGER–BORGESIUŞ–REYNA *i. m.* (pdf); HERNÁDI Júlia: *Privacy és fogyasztóvédelem*. In: RIGÓ Csaba Balázs – SZOBOSZLAI Izabella – CSIRSZKI Martin Milán (szerk.): *A hazai fogyasztóvédelmi jog áttekintése: alapok, kihívások, aktualitások*. Bp., GVH, 2023. 363–376.; LIBER Ádám: *Adatvédelem és platformok a DSA tükrében*. PhD-értekezés, Bp., 2025. https://lib.kre.hu:8080/phd/Liber_Adam_ertekezes.pdf (letöltés: 2026. 02. 03.); TÓTH András *i. m.* 24–34.

FELHASZNÁLT IRODALOM

Szakirodalmi források

ALMEIDA, Rui Filipe Gordete: *Os dados pessoais como contraprestação nos contratos de consumo — a necessidade para a execução do contrato como fundamento de licitude do tratamento* Personal data as counter-performance in consumer contracts — the necessity for the performance of a contract as a basis to ensure a lawful personal data processing. RED 2023/2. 1–48. DOI 10.24840/2182-9845_2023-0002_0002 (letöltés: 2025. 12. 30.)

BAK Márton Ferenc – BORDÁS Péter: *Reguláció – dereguláció: Kihívások és lehetőségek a digitális piacok szabályozásában*. In: GLAVANITS Judit – SZABÓ Tamás (szerk.): *Kiszolgáltatott csoportok a digitális világban: A digitalizáció jogalkotói és jogalkalmazói kihívásai*. Universitas–Győr Nonprofit Kft., 2024. 7–22.

BEDIR, Cemre: *Data as Counter-Performance: Yet Another Point Where Digital Content Contracts and the GDPR Conflict*. 2018. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3648092 (letöltés: 2025. 12. 29.)

BELÉNYESI Pál: *A digitális piacok időszerű versenyjogi vonatkozásai. A digitális piacokra vonatkozó joggyakorlat és a kapcsolódó joggazdasági megfontolások összehasonlítása az Egyesült Államokban és az Európai Unióban*. 2015. 10. 02. https://www.gvh.hu/data/cms1033315/12_Belenyesi_Pal_a_digitalis_piacok.pdf (letöltés: 2023. 02. 06.)

BENCZE Mátyás: *A viselkedéstudományok eredményeinek hasznosíthatósága a hazai fogyasztóvédelmi jog területén*. In: SZIKORA Veronika – ÁRVA Zsuzsanna (szerk.): *A fogyasztók védelmének új irányai és kihívásai a XXI. században*. Debrecen, Debreceni Egyetem Állam- és Jogtudományi Kar, 2018. 173–188.

BENCSIK András: *A versenyjog szerepe a fogyasztói érdekek védelmében*. Jura 2012/2. 27–38.

BENDIK Tamás: *A GDPR keletkezése és a magyar jogrendszerre gyakorolt hatás*. In: PÉTERFALVI Attila (szerk.): *Szemelvények az információs jogok felügyeletének elmúlt 25 évéből*. Bp., NAIH, 2020. 79–110.

BENKŐ Livia: *Magánszféra kontextusban: technológia, szakpolitika és a szociális élet integritása*. Információs Társadalom 2018/2. 124–128.

BERECZKI Tamás: *Sütihelyzet Franciaországban – Változóban a „cookie wall” szabályozói megítélése?* Blogbejegyzés. 2021. 04. 05. <https://www.dataprivacy.hu/?p=1899> (letöltés: 2022. 02. 23.)

BEUC: *Connected but unfairly treated. Consumer survey results on the fairness of the online environment*. 2023. szeptember. https://www.beuc.eu/sites/default/files/publications/BEUC-X-2023-113_Fairness_of_the_digital_environment_survey_results.pdf (letöltés: 2024. 12. 22.)

BEUC: *„Dark Patterns” and the EU Consumer Law Acquis: Recommendations for better enforcement and reform*. 2022. [beuc-x-2022-013_dark_patterns_paper.pdf](https://www.beuc.eu/sites/default/files/publications/BEUC-X-2022-013_dark_patterns_paper.pdf) (letöltés: 2023. 11. 03.)

BEYER Fülöp: *In situ adathozzáférési jogok.* <https://www.ludovika.hu/blogok/itkiblog/2023/02/23/in-situ-adathozzaferesi-jogok/> (letöltés: 2024. 01. 02.)

BOJNÁR Katinka: *Egy jelentős EUB-döntés margóján.* In: SZABÓ Endre Győző (szerk.): *Az Infotörvénytől a GDPR-ig.* Bp., Ludovika Egyetemi Kiadó, 2021. 79–101.

BORGESIU, Frederik J Zuiderveen – KRUIKEMEIER, Sanne – C BOERMAN, Sophie – HELBERGER, Natali: *Tracking Walls, Take-It-Or-Leave-It Choices, the GDPR, and the ePrivacy Regulation.* EDPL 2017/3. https://www.ivir.nl/publicaties/download/EDPL_2017_03.pdf (letöltés: 2018. 12. 05.)

BOROS Anita: *A web-sütik használatának adatvédelmi kérdései.* Pro Futuro 2020/3. 43–58. <https://doi.org/10.26521/PROFUTURO/2020/3/8746> (letöltés: 2022. 02. 23.)

BOTTA, Marco – WIEDEMANN, Klaus: *'The Interaction of EU Competition, Consumer, and Data Protection Law in the Digital Economy: The Regulatory Dilemma in the Facebook Odyssey.'* Antitrust Bulletin 2019/3. 428–446. <https://doi.org/10.1177/0003603X19863590> (letöltés: 2022. 10. 22.)

BÖRÖCZ István: *A személyes adatok védelmének bírósági gyakorlata Magyarországon.* Jura 2014/2. 176–184.

BÖRÖCZ István – SZŐKE Gergely László: *A beépített adatvédelem (Privacy by Design) elve.* Infokommunikáció és Jog 2013/3. 120–125.

CENTRE FOR STRATEGY AND EVALUATION SERVICES: *Study to support the Fitness Check of EU consumer law on digital fairness and the report on the application of the Modernisation Directive (EU) 2019/2161.* Final Report - Part 1. Közzétéve: 2024. október 04. https://commission.europa.eu/publications/study-support-fitness-check-eu-consumer-law-digital-fairness-and-report-application-modernisation_en?prefLang=hu&etrans=hu (letöltés: 2024. 12. 01.)

CRÉMER, Jacques – MONTJOYE, Yves-Alexandre de – SCHWEITZER, Heike: *A Competition Policy for the Digital Era.* European Commission. 2019. <https://euagenda.eu/upload/publications/untitled-257961-ea.pdf> (letöltés: 2023. 02. 06.)

CZAPÁRI Dóra – SZŐKE Gergely László: *Az adatvédelem és az adathasznosítás egyik kulcskérdése: a személyes adatok anonimizálása.* Jura 2022/4. 24–48.

DÉNESNÉ ORCSIK Judit: *2018-tól jön a modernebb, de szigorúbb adatvédelem.* Ügyvédvilág 2016/4. 13–14.

DARÁZS Lénárd: *Digitális fogyasztóvédelem európai perspektívában.* In: Salus vocalis. Csegöldi indulás – Győri érkezés. 81–92. DOI: 10.59199/salusvocalis.2023.10 (letöltés: 2024. 02. 12.)

DE ELIZALDE: F. *Fragmenting Consumer Law Through Data Protection and Digital Market Regulations: The DMA, the DSA, the GDPR, and EU Consumer Law*. Journal of Consumer Policy 2025/48. 355–389. <https://doi.org/10.1007/s10603-025-09584-3> (letöltés: 2025. 03. 02.)

DOCTOROW, Cory: *As Platforms Decay, Let's Put Users First*. EFF 2023. május 9. <https://www.eff.org/deeplinks/2023/04/platforms-decay-lets-put-users-first> (letöltés: 2025. 12. 20.)

DUDÁS Gábor – ZAVODNYIK József: *A személyes adat mint ellenszolgáltatás a digitális szolgáltatások nyújtására irányuló szerződésekben*. In: BODZÁSI Balázs (szerk.): *Gazdasági jogi és adójogi tanulmányok 2020*. Budapesti Corvinus Egyetem, 2020. 99–114.

ELI: *Guiding Principles for Automated Decision-Making in the EU*. ELI Innovation Paper. https://www.europeanlawinstitute.eu/fileadmin/user_upload/p_eli/Publications/ELI_Innovation_Paper_on_Guiding_Principles_for_ADM_in_the_EU.pdf (letöltés: 2025. 01. 03.)

ESZTERI Dániel: *Az új technológiák megjelenésének hatása a személyes adatok védelmére: gépi tanulás, blokklánc, internet-of-things, agyhullám-olvasás*. <https://real.mtak.hu/133906/1/eszteri.daniel.uj.technologiak.adatvedelem.pdf> (letöltés: 2022. 03. 02.)

FÉZER Tamás: *A fogyasztók adatainak és privátszférájának védelme elektronikus környezetben*. In: SZIKORA Veronika – ÁRVA Zsuzsanna (szerk.): *A fogyasztók védelmének új irányai és kihívásai a XXI. században*. Debrecen, Debreceni Egyetem Állam- és Jogtudományi Kar, 2018. 53–66.

FIRNIKSZ Judit: *Pillanatkép a digitális piacok szabályozásáról: A DMA a vállalati compliance tükrében*. Doktori értekezés. Bp., 2023

FURMAN, Jason et al.: *Unlocking Digital Competition, Report of the Digital Competition Expert Panel*. 2019. https://assets.publishing.service.gov.uk/media/5c88150ee5274a230219c35f/unlocking_digital_competition_furman_review_web.pdf (letöltés: 2024. 01. 02.)

FUSTER, Gloria González: *Article 18 Right to restriction of processing*. In: Christopher KUNER et. al: *The EU General Data Protection Regulation (GDPR): A Commentary*. 2020. 485–491. <https://academic.oup.com/oxford-law-pro/book/41324/chapter-abstract/352298156?redirectedFrom=fulltext&login=false> (letöltés: 2024. 01. 20.)

GCR (Global Competition Review): *Crucial Developments to European Data and Privacy in Merger Control*, 2023. december 08. <https://globalcompetitionreview.com/guide/digital-markets-guide/third-edition/article/crucial-developments-european-data-and-privacy-in-merger-control#footnote-009> (letöltés: 2024. 01. 12.)

GLAVANITS Judit: *A gazdasági folyamatok digitalizációjának egyes biztonsági és szabályozási kérdései*. Military and Intelligence CyberSecurity Research Paper 2023/6. 1–16.

GOANTA, Catalina – DE GREGORIO, Giovanni – SPANAKIS, Jerry: *Consumer Protection and Digital Vulnerability: Common and Diverging Paths*. In *The New Shapes of Digital Vulnerability in European Private Law*. 2024. 31–52. <https://www.nomos->

elibrary.de/10.5771/9783748940913-31/consumer-protection-and-digital-vulnerability-common-and-diverging-paths?page=3 (letöltés: 2025. 02. 02.)

GOMBOS Katalin: *A Digital Services Act és a Digital Markets Act várható kihívásai a jogalkalmazásban.* In: *Medias Res* 2023/2. 92–119.

GORECZKY Péter: *A határokon átnyúló adatáramlás gazdasági szempontjai.* 2024. [A határokon átnyúló adatáramlás gazdasági szempontjai - Világgazdaság \(vg.hu\)](https://vg.hu) (letöltés: 2024. 06. 02.)

GÖNCZÖL Tünde – TELEKI Lóránt: *A digitális kapuőrök az ex ante szabályozás, a versenyjog és az adatvédelem kerettüzeiben.* In: VALENTIN Pál et al. (szerk.): *Verseny és szabályozás, 2022.* Bp., MTA Közgazdaság- és Regionális Tudományi Kutatóközpont Közgazdaságtudományi Intézet, 2023. 243–265.

GRAFENSTEIN, Max von et al.: *Privacy icons as a component of effective transparency and controls under the GDPR: effective data protection by design based on art. 25 GDPR.* *Computer Law & Security Review: Volume 52, April 2024, 105924.* <https://doi.org/10.1016/j.clsr.2023.105924> (letöltés: 2025. 12. 28.)

G. KARÁCSONY Gergely: *Adatvédelmi szabályozás.* In: FARKAS Ádám – KELEMEN Roland (szerk.): *Kibertér és biztonság egyes jogtani és államtani kérdései.* Győr, Universitas-Győr Nonprofit Kft., 2024. 277–303.

G. KARÁCSONY Gergely: „Ideje megváltoztatni” – *Az arcfelismerő rendszerek alkalmazásának alapjogi kockázatai a közösségi média és a deepfake korában.* In: TÖRÖK Bernát – ZÓDI Zsolt (szerk.): *Az internetes platformok kora.* Bp., Ludovika Egyetemi Kiadó, 2022. 299–317.

HAJNAL Zsolt: *A digitális szolgáltatásokról szóló rendelet közvetítő szolgáltatókra vonatkozó új kötelezettségeiről, felelősségéről.* In: NEMESSÁNYI Zoltán (szerk.): *Nemzetközi magánjogi évkönyv.* 2024. Bp., Orac Kiadó, 2024. 142–159.

HAJNAL Zsolt: *A digitalizáció hatása a fogyasztóvédelmi jogalkotásra.* *Fontes Iuris* 2024/3–4. 41–48. <https://doi.org/10.51784/FI.2024.3-4.5> (letöltés: 2025. 07. 20.)

HAJNAL Zsolt: *A fogyasztói jogok egységes európai szabályozásának lehetséges irányai.* Doktori értekezés, Debrecen, 2013.

HAJNAL Zsolt: *A fogyasztói szerződések joga az Európai Unió jogában: közös alapok.* Debreceni Jogi Műhely 2014/1–2.

HAJNAL Zsolt: *A fogyasztóvédelem alanya: a fogyasztó.* In: SZIKORA Veronika (szerk.): *Magyar fogyasztóvédelmi magánjog – európai kitekintéssel.* Debrecen, Fogyasztóvédők Magyarországi Egyesülete, 2010. 39–52.

HAJNAL Zsolt: *A fogyasztóvédelem alapjai.* In: SZIKORA Veronika (szerk.): *Magyar fogyasztóvédelmi magánjog – európai kitekintéssel.* Debrecen, Fogyasztóvédők Magyarországi Egyesülete, 2010. 15–18.

HAJNAL Zsolt: *The New Liability Forms of Online Platforms in the New European Digital Legal Framework from the Consumers' Perspective*. Acta Universitatis Sapientiae Legal Studies 2023/2. 20–21.

HAJNAL Zsolt – GYŐRI Ágoston: *Az online platformok és piacterek felelőssége a DSA alapján*. In: KOLTAY András. *A vadnyugat vége?: Tanulmányok az Európai Unió platformszabályozásáról*. Bp., Orac Kiadó, 2024. 516–535.

HAJNAL Zsolt – SIMON Rita: *Key Challenges to the Implementation of the Digital Content Directive in Hungary and the Czech Republic*. In: Naděžda ŠIŠKOVÁ (szerk.): *Legal Issues of Digitalisation, Robotisation and Cyber Security in the Light of EU Law*. Praha, Kluwer Law International, 2024. 113–126.

HAN, Rong – JIANG, Na: *The integration of personal data protection into consumer law in EU digital markets*. Journal of Legal, Ethical and Regulatory Issues 2024/27. 1–6. <https://www.abacademies.org/articles/the-integration-of-personal-data-protection-into-consumer-law-in-eu-digital-markets-16802.html#r9> (letöltés: 2025. 01. 02.)

HÄUSELMANN, Andreas – CUSTERS, Bart: *The Right to Rectification and Inferred Personal Data*. European Journal of Law and Technology 2024/3. <https://ejlt.org/index.php/ejlt/article/view/1004/1097> (letöltés: 2025. 09. 08.)

HELBERGER, Natali et al.: *EU Consumer Protection 2.0: Structural asymmetries in digital consumer markets: A joint report from research conducted under the EUCP2.0 project*, 2021. március. https://www.beuc.eu/sites/default/files/publications/beuc-x-2021-018_eu_consumer_protection_2.0.pdf (letöltés: 2023. 12. 20.)

HELBERGER, Natali – BORGESIU, Frederik Zuiderveen – REYNA, Agustin: *The perfect match? A closer look at the relationship between EU Consumer Law and Data Protection Law*. Common Market Law Review 2017/5. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3048844 (letöltés: 2022. 10. 11.)

HERNÁDI Júlia: *Privacy és fogyasztóvédelem*. In: RIGÓ Csaba Balázs – SZOBOSZLAI Izabella – CSIRSZKI Martin Milán (szerk.): *A hazai fogyasztóvédelmi jog áttekintése: alapok, kihívások, aktualitások*. Bp., GVH, 2023. 363–376.

HOHMANN Balázs: *A Digital Services Act és a Digital Markets Act termékekre és digitális szolgáltatásokra irányuló fogyasztói jogviszonyokat érintő rendelkezései*. In Medias Res 2023/2. 69–91.

HORVÁTH M. András: *Sustainability and Competition Law in Hungary*. In: KÉLLEZI, Pranvera – KOBEL, Pierre – KILPATRICK, Bruce: *Sustainability Objectives in Competition and Intellectual Property Law* 2024. 127–161. <https://doi.org/10.1007/978-3-031-44869-0> (letöltés: 2025. 12. 30.)

JONG, Sander de – SPAGNUELO, Dayana: *Iconified Representations of Privacy Policies: a GDPR Perspective*. 2020. DOI:[10.1007/978-3-030-45691-7_75](https://doi.org/10.1007/978-3-030-45691-7_75) (letöltés: 2025. 12. 28.)

JÓRI András: *Az adatvédelmi jog generációi és egy második generációs szabályozás részletes elemzése*. PhD-dolgozat. Pécs, 2009. <https://ajk.pte.hu/files/file/doktori-iskola/jori-andras/jori-andras-vedes-ertekezes.pdf> (letöltés: 2022. 03. 04.)

KAPPEL Gergely – SIMON Soma: *Az elfeledtetéshez való jog – Európára korlátozva?* Arsboni 2020. február 17. <https://arsboni.hu/az-elfeledteteshez-valo-jog-europ/> (letöltés: 2021. 11. 22.)

KELLY, Eamonn: *Introduction: Business ecosystems come of age*. 2015. [Introduction: Business ecosystems come of age | Deloitte Insights | Business Trends](#) (letöltés: 2024. 02. 02.)

KELLY, Eamonn – MARCHESI, Kelly: *Supply chains and value webs*. 2015. [From supply chains to value webs | Deloitte Insights | Business Trends](#) (letöltés: 2024. 02. 02.);

KERBER, Wolfgang: *Competition Law in Context: The Example of its Interplay with Data Protection Law from an Economic Perspective*. *Wirtschaft und Wettbewerb* 2021/7–8. 400–404. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3890603 (letöltés: 2024. 02. 02.)

KERBER, Wolfgang – SPECHT-RIEMENSCHNEIDER, Louisa: *Synergies between data protection law and competition law*. 2021. szeptember 30. https://www.vzbv.de/sites/default/files/2021-11/21-11-10_Kerber_Specht-Riemenschneider_Study_Synergies_Between_Data%20protection_and_Competition_Law.pdf (letöltés: 2023. 02. 01.)

KERBER, Wolfgang – ZOLNA, Karsten K.: *The German Facebook case: the law and economics of the relationship between competition and data protection law*. *European Journal of Law and Economics* 2022/54. 217–250. <https://doi.org/10.1007/s10657-022-09727-8> (letöltés: 2024. 02. 02.)

KOOPS, Bert-Jaap – NEWELL, Bryce Clayton – TIMAN, Tjerk – ŠKORVÁNEK, Ivan – CHOKREVSKI, Tomislav – GALIČ, Maša: *A Typology of Privacy*. *University of Pennsylvania Journal of International Law* 38(2)/2017. 483–575. <https://scholarship.law.upenn.edu/cgi/viewcontent.cgi?article=1938&context=jil> (letöltés: 2023. 02. 02.)

KOPPÁNY Zsombor: *A GDPR piaci hatásai*. 2019. <https://arsboni.hu/a-gdpr-piaci-hatasai/> (letöltés: 2025. 12. 10.)

KOZMA Gábor Levente: *Quid pro quo: a személyes adat mint ellenszolgáltatás*. *Versenytükör* 2023. különszám. 76–88.

KOZMA Zoltán – ALMÁSY Márk: *Érvénytelen az EU–USA Adatvédelmi Pajzs – Az Európai Bíróság ítéletet hozott a kiemelt jelentőségű Schrems II ügyben*. [Érvénytelen az EU-USA Adatvédelmi Pajzs - Az Európai Bíróság ítéletet hozott a kiemelt jelentőségű Schrems II ügyben - Jogi Fórum](#) (letöltés: 2024. 02. 02.)

LARSSON, Stefan: *Algorithmic governance and the need for consumer empowerment in data-driven markets*. <https://policyreview.info/articles/analysis/algorithmic-governance-and-need-consumer-empowerment-data-driven-markets> (letöltés: 2018. 11. 25.)

LEISER, M. R.: *Illuminating Manipulative Design: from „Dark Patterns” to Information Asymmetry and the Repression of Free Choice under the Unfair Commercial Practices Directive*. 2022. 1–30. <http://dx.doi.org/10.2139/ssrn.4418586> (letöltés: 2024. 08. 04.)

LIBER Ádám: *Adatvédelem és platformok a DSA tükrében*. PhD-értekezés, Bp., 2025. https://lib.kre.hu:8080/phd/Liber_Adam_ertekezes.pdf (letöltés: 2026. 02. 03.)

LÖLFING, Nils: *CJEU confirms preparatory acts can be automated individual decisions: the SCHUFA cases*. Bird & Bird 2023. https://www.twobirds.com/en/insights/2023/global/key-takeaways-from-the-schufa-case-of-the-cjeu?utm_source=chatgpt.com (letöltés: 2025. 01. 05.)

MAJTÉNYI László: *Információs jogok*. In: HALMAI Gábor – TÓTH Gábor Attila (szerk.): *Emberi jogok*. Bp., Osiris, 2003. 576–735.

MATHUR, Arunesh – MAYER, Jonathan – KSHIRSAGAR, Mihir: *What Makes a Dark Pattern... Dark? Design Attributes, Normative Considerations, and Measurement Methods*. Proceedings of the 2021 CHI Conference on Human Factors in Computing Systems, 2021. <https://doi.org/10.1145/3411764.3445610> (letöltés: 2023. 12. 21.)

MENYHÁRD Attila: *A magánélethez való jog elméleti alapjai*. In *Medias Res* 2014/2. 384–406.

MENYHÁRD Attila: *A platformok polgári jogi felelőssége*. In: TÖRÖK Bernát – ZÓDI Zsolt (szerk.): *Az internetes platformok kora*. Bp., Ludovika Egyetemi Kiadó, 2022. 129–148.

MEZEI Kitti – TRÄGER Anikó: *Kockázatok és reziliencia az online platformok és a mesterséges intelligencia európai uniós szabályozásában*. MTA Law Working Papers 2024/1. <https://jog.tk.hun-ren.hu/mtalwp/kockazatok-es-reziliencia-az-online-platformok-es-a-mesterseges-intelligencia-europai-unios-szabalyozasaban> (letöltés: 2024. 09. 11.)

MICKLITZ, Hans-W.: *Dissolution of EU consumer law through fragmentation and privatisation*. In: HELBERGER, Natali et al.: *Digital fairness for consumers*. 2024. 71–144.

MIKLÓS Gellért: *Az Európai Unió adatstratégiájához kapcsolódó jogszabályi keretrendszer áttekintése*. Századvég 2022/1. 69–94.

MURGIA, Madhumita – ESPINOZA, Javier: *Ireland is ‘worst bottleneck’ for enforcing EU data privacy law – ICCL Report says Irish data protection watchdog failing to take action against US tech giants*. 2021. szeptember 13. <https://www.irishtimes.com/business/technology/ireland-is-worst-bottleneck-for-enforcing-eu-data-privacy-law-iccl-1.4672480> (letöltés: 2023. 02. 02.)

NAMYSŁOWSKA, Monika: *Future-Proofing the Unfairness Test*. In: Natali HELBERGER et al.: *Digital fairness for consumers*. 2024. 163–241. https://www.beuc.eu/sites/default/files/publications/BEUC-X-2024-032_Digital_fairness_for_consumers_Report.pdf (letöltés: 2025. 03. 02.)

NAMYSŁOWSKA, M.: *The Silent Death of EU Consumer Law and Its Resilient Revival: Reinventing Consumer Protection Against Unfair Digital Commercial Practices*. *Journal of Consumer Policy* 2025/48. 317–336. <https://doi.org/10.1007/s10603-025-09590-5> (letöltés: 2025. 12. 22.)

OECD: *Toolkit for protecting digital consumers: A Resource for G20 Policy Makers*. 2018. <https://www.consumatoriumbria.it/wp-content/uploads/2024/05/toolkit-for-protecting-digital-consumers-OEDC.pdf> (letöltés: 2022. 02. 02.)

OSZTOVITS András: *A technológia hálójában – a magánjogi jogérvényesítés jelene és lehetséges jövője*. In: ZÖDI Zsolt (szerk.): *Jogi technológiák: Digitális jogalkalmazás*. Bp., Ludovika Egyetemi Kiadó, 2022. 285–301.

PESSOA, Rafael: *Is an Icon Worth a Thousand Words? Grounded Legal Strategies for Standardised Icons Under the GDPR*. Tilburg Law School Tilburg Institute for Law, Technology, and Society 2023. július. <https://arno.uvt.nl/show.cgi?fid=162909> (letöltés: 2025. 12. 28.)

PÉTERFALVI Attila: *Az adatvédelem fejlődésének történeti áttekintése Magyarországon a GDPR hatálybalépéséig*. In: PÉTERFALVI Attila (szerk.): *Szemelvények az információs jogok felügyeletének elmúlt 25 évéből*. Bp., NAIH, 2020. 29–78.

PÉTERFALVI Attila – RÉVÉSZ Balázs – BUZÁS Péter (szerk.): *Magyarázat a GDPR-ról*. Bp., Wolters Kluwer Hungary, 2021

PETRÁNYI Dóra – DOMOKOS Márton – HORVÁTH Anna Zsófia – HUSZÁR Daniella: *Az online platformokon alkalmazott sötét megoldások*. 2023. július 4. <https://onlineplatformok.hu/files/21982413-9a9f-4e6f-b6b5-2530bda6d7ed.pdf> (letöltés: 2024. 01. 01.)

PÓK László: *Adalékok a közös adatkezelés megállapításához*. Blogbejegyzés, 2024. március 08. https://gdpr.blog.hu/2024/03/08/adalekok_a_kozos_adatkezeles_megallapitasahoz (letöltés: 2024. 08. 21.)

PÓK László: *Az adatvédelem „szuperalapelve” – az elszámoltathatóság*. Blogbejegyzés. 2017. június 14. http://gdpr.blog.hu/2017/06/14/az_adatvedelem_szuperalapelve_az_elszamoltathatosag (letöltés: 2018. 05. 03.)

PÓK László: *Az Európai Bíróság újabb Meta-ügyben hozott döntése: bajban az online hirdetési szektor?* Blogbejegyzés, 2023. július 7. https://gdpr.blog.hu/2023/07/07/az_europai_birosag_ujabb_meta-ugyen_hozott_dontese_bajban_az_online_hirdetesi_szektor (letöltés: 2024. 02. 02.)

PÓK László: *Egy kis lépés a személyes adat fogalmának relatív(abb) értelmezése felé?* Blogbejegyzés. 2023. november 15. https://gdpr.blog.hu/2023/11/15/egy_kis_lepes_a_szemelyes_adat_fogalmanak_relativ_ertelmeseze_fele (letöltés: 2023. 12. 10.)

POLYÁK Gábor – PATAKI Gábor: *A személyes adatok értéke a Facebook–WhatsApp-összefonódás versenyjogi értékelésében*. Pro Futuro 2018/1. 131–147.

PURTOVA, Nadezsda: *The law of everything. Broad concept of personal data and future of EU data protection law*. Law, Innovation and Technology 2018/10. 40–81. <https://doi.org/10.1080/17579961.2018.1452176> (letöltés: 2023. 12. 20.)

PUSZTAHELYI Réka: *A személyes adatok üzleti célú megszerzésére alkalmazott „sötét minták” elleni fellépés lehetséges formái.* In *Medias Res* 2023/2. 158–161.

PÜNKÖSTY András: *A nagy adathalmazok felhasználásának etikai kérdései – avagy szükség van-e adatetikára?* In: TÖRÖK Bernát – ZÖDI Zsolt: *Digitalizálódó társadalom: Tanulmányok az új technológiák társadalmi-jogi hatásairól.* Bp., Ludovika Egyetemi Kiadó, 2023. 215–233.

RHOEN, Michiel: *Beyond consent: improving data protection through consumer protection law.* *Internet Policy Review* 2016/1. <https://doi.org/10.14763/2016.1.404> (letöltés: 2018. 02. 02.)

ROSE, John – REHSE, Olaf – RÖBER, Björn: *Related: The Value of Our Digital Identity.* <https://www.bcg.com/en-hu/publications/2012/digital-economy-consumer-insight-value-of-our-digital-identity.aspx> (letöltés: 2018. 11. 30.)

SAHLSTEDT, Andreas: *A competition policy for the digital age – An analysis of the challenges posed by data- driven business models to EU competition law.* Uppsala Universitet, 2019. <http://bit.ly/37EAnNM> (letöltés: 2019. 01. 14.)

SAX, Marijn – HELBERGER, Natali: *Digital Vulnerability and Manipulation in the Emerging Digital Framework.* In: Natali HELBERGER et al.: *Digital fairness for consumers.* 2024. 11–24.

SIMON Éva: *Egy XIX. századi tanulmány margójára.* *Információs Társadalom* 2005/2. 32–43.

SÓLYOM László: *A személyiségi jogok elmélete.* Bp., Közgazdasági és Jogi Könyvkiadó, 1983.

SÓLYOM László: *Egy új szabadságjog: az információszabadság.* *Valóság* 1988/9. 14–34.

SÖRENSEN, Ove: *Zombie-cookies: Case studies and mitigation.* London, IEEE. 321–326. [doi: 10.1109/ICITST.2013.6750214](https://doi.org/10.1109/ICITST.2013.6750214) (letöltés: 2022. 10. 21.)

SZABÓ Endre Győző: *Az Európai Unió általános adatvédelmi rendeletének egyes kérdéseiről, II.: Beépített és alapértelmezett adatvédelem – Adatvédelmi incidensek bejelentése.* Pázmány Law Working Papers 2016/27. https://plwp.eu/docs/wp/2016/2016-27_Szabo.pdf (letöltés: 2019. 01. 04.)

SZABÓ Máté Dániel: *Kísérlet a Privacy fogalmának meghatározására a magyar jogrendszer fogalmaival.* *Információs Társadalom* 2005/2. 44–54.

SZEGEDI László – DORNFELD László – POLGÁR Zoltán – TELEKI Bálint: *A GDPR alkalmazásával kapcsolatos első tagállami tapasztalatok – Egységes szabályozás, eltérő alkalmazás?* *Infokommunikáció és Jog* 2021/1. 10–16.

SZOMMER Károly – BALOGH Zoltán – RACSKÓ Péter: *Az on-line világban hagyott virtuális lábnyomokban rejlő információk és azok veszélyei.* *Vezetéstudomány* 2014/7–8. 97–104.

SZŐKE Gergely László: *Az adatvédelem szabályozásának történeti áttekintése.* *Infokommunikáció és Jog* 2013/3. 107–112.

SZŐKE Gergely László: *Az európai adatvédelmi jog megújítása. Tendenciák és lehetőségek az önszabályozás területén.* (PhD-értékezés), Pécs (2014). <https://ajk.pte.hu/files/file/doktori-iskola/szoke-gergely-laszlo/szoke-gergely-laszlo-vedes-ertekezes.pdf.pdf> (letöltés: 2018. 12. 05.)

TÓTH András: *A Digital Services Act és az EU fogyasztóvédelmi joga.* KözigazgatásTudomány 2023/2. 24–34. <https://doi.org/10.54200/kt.v3i2.67> (letöltés: 2024. 02. 02.)

TÓTH András: *A technológiai óriások piaci megregulázásának versenyjogi mozgatói és aspektusai, különös tekintettel a Digital Markets Act javaslatra.* VersenyTükör 2021/1. 37–54.

TÓTH András: *Az adatmonopóliumok tündöklése és letörése.* In: SZABÓ Endre Győző: *Az Infotörvénytől a GDPR-ig.* Bp., Ludovika Egyetemi Kiadó, 2021. 161–184.

TÓTH András: *Fogyasztóvédelmi, adatvédelmi, médiajogi és versenyjogi eszközök együttes alkalmazása az online figyelempiacok kudarcainak kiküszöbölésére.* Infokommunikáció és Jog 2021/2. 8–14.

TÓTH András – SZABÓ Endre Győző – NÉMETH Szabolcs – RUDICS Regina – RIDEG Gergely: *A GDPR és a Digital Markets Act viszonyának tisztázása.* In *Medias Res* 2023/2. 45–68.

TÓTH Tihamér: *Fogyasztóvédelmi közjog.* Egyetemi jegyzet és szöveggyűjtemény. Pécs, 2017. <https://jak.ppke.hu/uploads/articles/12239/file/Fogyik%C3%B6zjogjegyzet%20-%20T%C3%B3th%20Tiham%C3%A9r.pdf> (letöltés: 2023. 01. 03.)

TÖRÖK Bernát: *Az „empíria-feletti” ember.* Jogtudományi Közlöny 2025/12. 530–538. <https://doi.org/10.59851/jk.80.12.3> (letöltés: 2026. 01. 02.)

TÖRÖK Éva: *A fogyasztói szerződésekkel kapcsolatos jogalkalmazás – különös tekintettel az egyértelmű megfogalmazás követelményére.* In: SZIKORA Veronika – ÁRVA Zsuzsanna (szerk.): *A fogyasztók védelmének új irányai és kihívásai a XXI. században.* Debrecen, Debreceni Egyetem Állam- és Jogtudományi Kar (2018). 67–81.

TRSTENJAK, Verica: *GDPR as a New Consumer Protection “Weapon”?* European Studies – the Review of European law, Economics and Politics 2024/2. 15–32. DOI: 10.2478/eustu-2024-0014 (letöltés: 2025. 12. 30.)

VANDE WALLE, Simon: *The European Commission Clears the Acquisition of a Maker of Fitness Trackers and Smartwatches by a Major Online Platform, Subject to Long-Lasting Behavioural Remedies* (Google/Fitbit, M.9660) (September 2, 2021). *Concurrences Competition Law Review* 2021/3. <https://ssrn.com/abstract=3915946> (letöltés: 2024. 02. 02.)

VIKMAN László: *Direktmarketing és spam – lehetőségek, korlátok,* https://www.jogiforum.hu/files/publikaciok/vikman_laszlo_dm-spam%5bjogi_forum%5d.pdf (letöltés: 2019. 06. 02.)

WAERDT, Peter J. van de: *Information asymmetries: recognizing the limits of the GDPR on the data-driven market.* Computer Law & Security Review 2020/38. <https://doi.org/10.1016/j.clsr.2020.105436> (letöltés: 2022. 03. 03.)

WARREN, Samuel D. – BRANDEIS, Louis D.: *A magánszférához való jog*. Információs Társadalom 2005/2. 7–31.

ZÖDI Zsolt: *A platform mint elméleti konstrukció és mint narratív keret – A platformfogalom kialakulásának története*. In: TÖRÖK Bernát – ZÖDI Zsolt (szerk.): *Az internetes platformok kora*. Bp., Ludovika Egyetemi Kiadó, 2022. 17–38.

ZÖDI Zsolt: *A platformszabályozás megold(hat)atlan dilemmái*. In: TÖRÖK Bernát – ZÖDI Zsolt: *Digitalizálódó társadalom: Tanulmányok az új technológiák társadalmi-jogi hatásairól*. Bp., Ludovika Egyetemi Kiadó 2023. 81–101.

ZÖDI Zsolt: *Az európai platformszabályozás jellegzetességei: Platformjog és felhasználóvédelem*. In *Medias Res* 2022/1. 66–82.

Zödi Zsolt: *Jog és jogtudomány a Big Data korában*. Állam- és Jogtudomány 2017/1. 95–114.

ZÖDI Zsolt: *Platformok, robotok és a jog*. Bp., Gondolat, 2018

Zödi Zsolt: *Privacy és a Big Data*. Fundamentum 2017/1–2. 18–30.

32nd International Conference of Data Protection and Privacy Commissioners Jerusalem, Israel 27-29 October, 2010. Resolution on Privacy by Design. <https://globalprivacyassembly.org/wp-content/uploads/2015/02/32-Conference-Israel-resolution-on-Privacy-by-Design.pdf> (letöltés: 2022. 01. 12.)

Európai uniós és nemzetközi jogszabályok

A Bizottság (EU) 2023/1795 végrehajtási határozata (2023. július 10.) az (EU) 2016/679 európai parlamenti és tanácsi rendelet szerint a személyes adatoknak az EU–USA adatvédelmi keret által biztosított megfelelő szintű védelméről

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 szóló, 2016. április 27-i (EU) 2016/680 európai parlamenti és tanácsi irányelv

A Tanács 139/2004/EK rendelete (2004. január 20.) a vállalkozások közötti összefonódások ellenőrzéséről (az EK összefonódás-ellenőrzési rendelete)

A Tanács 93/13/EGK irányelve (1993. április 5.) a fogyasztókkal kötött szerződésekben alkalmazott tisztességtelen feltételekről

Az egyének védelméről a személyes adatok gépi feldolgozása során, Strasbourgban, 1981. január 28. napján kelt egyezmény

Az Emberi Jogok Egyetemes Nyilatkozata

Az emberi jogok és az alapvető szabadságok védelméről szóló, Rómában, 1950. november 4-én kelt egyezmény

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 1215/2012/EU rendelete (2012. december 12.) a polgári és kereskedelmi ügyekben a joghatóságról, valamint a határozatok elismeréséről és végrehajtásáról

Az Európai Parlament és a Tanács 593/2008/EK rendelete (2008. június 17.) a szerződéses kötelezettségekre alkalmazandó jogról

Az Európai Parlament és a Tanács (EU) 2015/2302 irányelve (2015. november 25.) az utazási csomagokról és az utazási szolgáltatáseggyüttesekről, valamint a 2006/2004/EK rendelet és a 2011/83/EU európai parlamenti és tanácsi irányelv módosításáról, továbbá a 90/314/EGK tanácsi irányelv hatályon kívül helyezéséről

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

Az Európai Parlament és a Tanács (EU) 2018/1725 rendelete (2018. október 23.) a természetes személyeknek a személyes adatok uniós intézmények, szervek, hivatalok és ügynökségek általi kezelése tekintetében való védelméről és az ilyen adatok szabad áramlásáról, valamint a 45/2001/EK rendelet és az 1247/2002/EK határozat hatályon kívül helyezéséről

Az Európai Parlament és a Tanács (EU) 2018/302 rendelete (2018. február 28.) a belső piacon belül a vevő állampolgársága, lakóhelye vagy letelepedési helye alapján történő indokolatlan területi alapú tartalomkorlátozással és a megkülönböztetés egyéb formáival szembeni fellépésről, valamint a 2006/2004/EK és az (EU) 2017/2394 rendelet, továbbá a 2009/22/EK irányelv módosításáról

Az Európai Parlament és a Tanács (EU) 2019/1150 rendelete (2019. június 20.) az online közvetítő szolgáltatások üzleti felhasználói tekintetében alkalmazandó tisztességes és átlátható feltételek előmozdításáról

Az Európai Parlament és a Tanács (EU) 2019/770 irányelve (2019. május 20.) a digitális tartalom szolgáltatására és digitális szolgáltatások nyújtására irányuló szerződések egyes vonatkozásairól

Az Európai Parlament és a Tanács (EU) 2020/1828 irányelve (2020. november 25.) a fogyasztók kollektív érdekeinek védelmére irányuló képviseleti keresetekről és a 2009/22/EK irányelv hatályon kívül helyezéséről

Az Európai Parlament és a Tanács (EU) 2022/1925 rendelete (2022. szeptember 14.) a digitális ágazat vonatkozásában a versengő és tisztességes piacokról, valamint az (EU) 2019/1937 és az (EU) 2020/1828 irányelv módosításáról

Az Európai Parlament és a Tanács (EU) 2022/2065 rendelete (2022. október 19.) a digitális szolgáltatások egységes piacáról és a 2000/31/EK irányelv módosításáról

Az Európai Parlament és a Tanács (EU) 2023/988 rendelete (2023. május 10.) az általános termékbiztonságról, az 1025/2012/EU európai parlamenti és tanácsi rendelet és az (EU) 2020/1828 európai parlamenti és tanácsi irányelv módosításáról, valamint a 2001/95/EK európai parlamenti és tanácsi irányelv és a 87/357/EGK tanácsi irányelv hatályon kívül helyezéséről

Az Európai Parlament és a Tanács (EU) 2023/2225 irányelve (2023. október 18.) a fogyasztói hitelmegállapodásokról és a 2008/48/EK irányelv hatályon kívül helyezéséről

Az Európai Parlament és a Tanács (EU) 2023/2854 rendelete (2023. december 13.) a méltányos adathozzáférésre és -felhasználásra vonatkozó harmonizált szabályokról, valamint az (EU) 2017/2394 rendelet és az (EU) 2020/1828 irányelv módosításáról

Az Európai Parlament és a Tanács (EU) 2024/2853 irányelve (2024. október 23.) a hibás termékekért való felelősségről és a 85/374/EGK tanácsi irányelv hatályon kívül helyezéséről

Az Európai Parlament és a Tanács (EU) 2024/825 irányelve (2024. február 28.) a 2005/29/EK és a 2011/83/EU irányelv módosításáról, a fogyasztók zöld átállásban való szerepvállalásának a tisztességtelen gyakorlatokkal szembeni hatékonyabb védelem és a hatékonyabb tájékoztatás révén történő növelése tekintetében

Az Európai Parlament és a Tanács (EU) 2025/2518 rendelete (2025. november 26.) az (EU) 2016/679 rendelet végrehajtására vonatkozó további eljárási szabályok megállapításáról

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 2005/29/EK irányelve a belső piacon az üzleti vállalkozások fogyasztókkal szemben folytatott tisztességtelen kereskedelmi gyakorlatairól, valamint a 84/450/EGK tanácsi irányelv, a 97/7/EK, a 98/27/EK és a 2002/65/EK európai parlamenti és tanácsi irányelvek, valamint a 2006/2004/EK európai parlamenti és tanácsi rendelet módosításáról

Az Európai Parlament és a Tanács 2006/24/EK irányelve (2006. március 15.) a nyilvánosan elérhető elektronikus hírközlési szolgáltatások nyújtása, illetve a nyilvános hírközlő hálózatok szolgáltatása keretében előállított vagy feldolgozott adatok megőrzéséről és a 2002/58/EK irányelv módosításáról. Hatályos 2006. 05. 03-ig.

Az Európai Parlament és a Tanács 2009/136/EK irányelve (2009. november 25.) az egyetemes szolgáltatásról, valamint az elektronikus hírközlő hálózatokhoz és elektronikus hírközlési szolgáltatásokhoz kapcsolódó felhasználói jogokról szóló 2002/22/EK irányelv, az elektronikus hírközlési ágazatban a személyes adatok kezeléséről, feldolgozásáról és a magánélet védelméről szóló 2002/58/EK irányelv és a fogyasztóvédelmi jogszabályok alkalmazásáért felelős nemzeti hatóságok közötti együttműködésről szóló 2006/2004/EK rendelet módosításáról

Az Európai Parlament és a Tanács 2011. október 25-i 2011/83/EU irányelve a fogyasztók jogairól, a 93/13/EGK tanácsi irányelv és az 1999/44/EK európai parlamenti és tanácsi irányelv

módosításáról, valamint a 85/577/EGK tanácsi irányelv és a 97/7/EK európai parlamenti és tanácsi irányelv hatályon kívül helyezéséről

Az Európai Parlament és a Tanács 2013/37/EU irányelve (2013. június 26.) a közsféra információinak további felhasználásáról szóló 2003/98/EK irányelv módosításáról

Az Európai Parlament és a Tanács 2019/2161 irányelve (2019. november 27.) a 93/13/EGK tanácsi irányelvnek, valamint a 98/6/EK, a 2005/29/EK és a 2011/83/EU európai parlamenti és tanácsi irányelvnek az uniós fogyasztóvédelmi szabályok hatékonyabb végrehajtása és korszerűsítése tekintetében történő módosításáról

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

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

Az Európai Unió alapjogi chartája

Az Európai Unió működéséről szóló szerződés 169. cikk

OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data (1980). Kivonatos magyar nyelvű fordítása: Áttekintés: OECD Irányelvek a magánélet védelméről és a személyes adatok határokon átvéelő áramlásáról

Magyar jogszabályok

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

1996. évi LVII. törvény a tisztességtelen piaci magatartás és a versenykorlátozás tilalmáról

1997. évi CLV. törvény a fogyasztóvédelemről

2003. évi C. törvény az elektronikus hírközlésről

2008. évi XLVII. törvény a fogyasztókkal szembeni tisztességtelen kereskedelmi gyakorlat tilalmáról

2008. évi XLVIII. törvény a gazdasági reklámtevékenység alapvető feltételeiről és egyes korlátairól

2011. évi CXII. törvény az információs önrendelkezési jogról és az információszabadságról

2013. évi V. törvény a Polgári Törvénykönyvről

2019. évi XXXIV. törvény az Európai Unió adatvédelmi reformjának végrehajtása érdekében szükséges törvénymódosításokról

45/2014. (II. 26.) Korm. rendelet a fogyasztó és a vállalkozás közötti szerződések részletes szabályairól

472/2017. (XII. 28.) Korm. rendelet az utazási szolgáltatásokra vonatkozó szerződésekről, különösen az utazási csomagra és az utazási szolgáltatás együttesre vonatkozó szerződésekről

EUB-ítéletek

ECLI:EU:C:1994:34. A Bíróság (ötödik tanács) ítélete a C-315/92. sz. ügyben (Verband Sozialer Wettbewerb eV kontra Clinique Laboratoires SNC et Estée Lauder Cosmetics GmbH), 1994. február 2.

ECLI:EU:C:2000:8. A Bíróság (ötödik tanács) ítélete a C-220/98. sz. ügyben (Estée Lauder Cosmetics GmbH & Co. OHG v Lancaster Group GmbH), 2000. január 13.

ECLI:EU:C:2014:237. A Bíróság ítélete (nagytanács) a C-288/12. sz. ügyben (Bizottság kontra Magyarország, kötelezettségszegés), 2014. április 8.

ECLI:EU:C:2014:238. A Bíróság ítélete (nagytanács) a C-293/12. és C-594/12. sz. egyesített ügyekben (2006/24/EK irányelv érvényessége), 2014. április 8.

ECLI:EU:C:2014:317. A Bíróság ítélete (nagytanács) a C-131/12. sz. ügyben (spanyol Google és Mario Costeja González), 2014. május 13.

ECLI:EU:C:2015:639. A Bíróság ítélete (harmadik tanács) a C-230/14. sz. ügyben (Weltimmo és NAIH), 2015. október 1.

ECLI:EU:C:2017:321. A Bíróság végzése (tizedik tanács) a C-535/16. sz. ügyben (Michael Tibor Bachman kontra FAER IFN SA), 2017. április 27.

ECLI:EU:C:2019:801. A Bíróság ítélete (nagytanács) a C-673/17. sz. ügyben (Cookie-k, előre bejelölt négyzettel megadott hozzájárulás), 2019. október 1.

ECLI:EU:C:2020:263. A Bíróság ítélete (első tanács) a C-329/19. sz. ügyben (Condominio di Milano, via Meda és az Eurothermo SpA ügy), 2020. április 2.

ECLI:EU:C:2020:559. A Bíróság ítélete (nagytanács) a C-311/18. sz. ügyben (az EU–USA adatvédelmi pajzs által biztosított védelem megfeleltetése), 2020. július 16.

ECLI:EU:C:2021:483. A Bíróság ítélete (nagytanács) a C-645/19. sz. ügyben (belga adatvédelmi hatóság kontra Facebook), 2021. június 15.

ECLI:EU:C:2023:537. A Bíróság ítélete (nagytanács) a C-252/21. sz. ügyben (Facebook kontra Bundeskartellamt), 2023. július 4.

ECLI:EU:C:2023:837. A Bíróság ítélete (harmadik tanács) a C-319/22. sz. ügyben (alkatrész-kereskedők kontra Scania), 2023. november 9.

ECLI:EU:C:2023:957. A Bíróság (első tanács) ítélete a C-634/21. sz. ügyben (SCHUFA, automatizált döntéshozatal hitelminősítésnél), 2023. december 7.

ECLI:EU:C:2024:214. A Bíróság ítélete (negyedik tanács) a C-604/22. sz. ügyben (IAB Europe és Gegevensbeschermingsautoriteit), 2024. március 7.

ECLI:EU:C:2024:846. A Bíróság ítélete (nagytanács) a C-21/23. sz. ügyben (gyógyszerek forgalmazása online platformon), 2024. október 4.

ECLI:EU:C:2025:2. A Bíróság ítélete (első tanács) a C-394/23. sz. ügyben (a megszólításra vonatkozó adatok), 2025. január 9.

ECLI:EU:C:2025:172. A Bíróság ítélete (első tanács) a C-247/23. sz. Deldits-ügyben (helyesbítéshez való jog a nemi identitásra vonatkozóan), 2025. március 13.

Egyéb ítéletek

15/1991. (IV. 13.) AB határozat

BVerfG. Az Első Szenátus 1983. december 15-i végzése - 1 BvR 209/83

PS6980. Autorità Garante della Concorrenza e del Mercato, 2013. november 06.

Fővárosi Közigazgatási és Munkaügyi Bíróság: 13.K.32.793/2016/15.

Fővárosi Törvényszék: 105.K.701.043/2020/14.

Kúria: Kfv.II.37.243/2021/11.

BH 2025.1.13.

Versenyügyek

AT.39740. sz. ügy – Google Search (Shopping)

AT.40670. sz. ügy – Google

AT.40684. sz. ügy – Facebook–Marketplace

C-252/21. sz. ügy – Meta Platforms/Bundeskartellamt

M.4731. sz. ügy – Google–DoubleClick

M.7217. sz. ügy – Facebook/WhatsApp

M.8228. sz. ügy – Facebook/WhatsApp

M.9660. sz. ügy – Google/Fitbit

Bundeskartellamt B6-22/16. sz. határozata, 2019. február 06. (Meta Platforms/Bundeskartellamt ügy)

GVH-ügyek

VJ/28-61/2022.

Vj-3/2020/247.

Vj-85/2016/189.

Vj-88/2016/71.

NAIH-dokumentumok

NAIH/2016/2504/27/H

NAIH/2017/491/H

NAIH/2018/3567/2/V

NAIH-2264-2/2014/J

NAIH-2857-20/2021

NAIH-3195-11/2022

NAIH STAR-projekt: 1. témakör – Bevezetés az uniós adatvédelmi rendszerbe. 7. témakör – Technikai és szervezési intézkedések. <https://www.naih.hu/star-i/stari-eredmenyek> (letöltés: 2023. 02. 02.)

NAIH: *Adatvédelmi értelmező szótár*. <https://www.naih.hu/adatvedelmi-szotar> (letöltés: 2023. 01. 01.)

NAIH: GDPR 35. cikk (4) bekezdése alapján összeállított jegyzék: https://naih.hu/files/GDPR_35_4_lista_HU_mod.pdf (letöltés: 2022. 03. 02.)

A 29. cikk alapján létrehozott munkacsoport és az EDPB dokumentumai

WP136. A 29. cikk alapján létrehozott adatvédelmi munkacsoport: 4/2007. vélemény a személyes adat fogalmáról

Wp168. Article 29 Data Protection Working Party: The Future of Privacy. Joint contribution to the Consultation of the European Commission on the legal framework for the fundamental right to protection of personal data. Adopted on 01 December 2009.

WP171. A 29. cikk alapján létrehozott adatvédelmi munkacsoport: 2/2010. számú vélemény a viselkedésalapú online reklámról. Elfogadás időpontja: 2010. június 22.

WP194. A 29. cikk szerinti adatvédelmi munkacsoport: 2012/4. számú vélemény a sütikhez való hozzájárulás alóli mentességről. Elfogadás időpontja: 2012. június 7.

WP216. 29. cikk alapján létrehozott adatvédelmi munkacsoport: 05/2014. számú vélemény az anonimizálási technikákról

WP217. A 29. cikk szerinti munkacsoport: 06/2014. számú vélemény az adatkezelő 95/46/EK irányelv 7. cikke szerinti jogszerű érdekeinek fogalmáról. Elfogadás időpontja: 2014. április 9.

WP242. A 29. cikk szerinti munkacsoport: Iránymutatás az adatok hordozhatóságáról. A legutóbbi felülvizsgálat és elfogadás időpontja: 2017. április 5.

WP248. A 29. cikk alapján létrehozott adatvédelmi munkacsoport: Iránymutatás az adatvédelmi hatásvizsgálat elvégzéséhez és annak megállapításához, hogy az adatkezelés az (EU) 2016/679 rendelet alkalmazásában „valószínűsíthetően magas kockázattal jár”-e

WP251. A 29. cikk szerinti adatvédelmi munkacsoport: Iránymutatás az automatizált döntéshozatallal és a profilalkotással kapcsolatban a 2016/679 rendelet alkalmazásához. A legutóbbi felülvizsgálat és elfogadás időpontja: 2018. február 6.

WP259. A 29. cikk szerinti adatvédelmi munkacsoport: A 29. cikk szerinti munkacsoport iránymutatása az (EU) 2016/679 rendelet szerinti hozzájárulásról. Utolsó felülvizsgált és elfogadott változat időpontja: 2018. április 10.

WP260. A 29. CIKK SZERINTI ADATVÉDELMI MUNKACSOPORT: Iránymutatás az (EU) 2016/679 rendelet szerinti átláthatóságról. A legutóbbi felülvizsgálat és elfogadás időpontja: 2018. április 11.

EDPB: 02/2022. sz. iránymutatás az általános adatvédelmi rendelet 60. cikkének alkalmazásáról. 1.1. verzió. Elfogadva: 2022. március 14.

EDPB: 03/2021. nyilatkozat az elektronikus hírközlési adatvédelmi rendeletről. Elfogadás időpontja: 2021. március 9.

EDPB: 07/2020. sz. iránymutatás az adatkezelő és az adatfeldolgozó GDPR szerinti fogalmáról 2.0 változat. Elfogadás időpontja: 2021. július 7.

EDPB: 11/2024. sz. vélemény a repülőtéri utasforgalom egyszerűsítése érdekében az arcfelismerés alkalmazásáról (összeegyeztethetőség az általános adatvédelmi rendelet 5. cikke (1) bekezdésének e) és f) pontjával, valamint 25. és 32. cikkével) 1.1. verzió. Elfogadás időpontja: 2024. május 23.

EDPB: 2/2019. iránymutatás a személyes adatoknak az általános adatvédelmi rendelet 6. cikke (1) bekezdésének b) pontja szerinti kezeléséről az érintettek részére nyújtott online szolgáltatások összefüggésében. 2.0 változat. 2019. október 8.

EDPB: 2024/08. sz. vélemény az érvényes hozzájárulásról a nagy online platformok által alkalmazott, hozzájárulást vagy díjfizetést megkövetelő modellekkel összefüggésben. Az elfogadás időpontja: 2024. április 17.

EDPB: 3/2018. sz. iránymutatás az általános adatvédelmi rendelet területi hatályáról (3. cikk) 2.1 változat. 2019. november 12.

EDPB: 03/2022. számú iránymutatás a közösségimédia-platformok interfészein előforduló megtévesztő tervezési megoldásokról: hogyan ismerjük fel és kerüljük el őket 2.0. változat. Az elfogadás időpontja: 2023. február 14.

EDPB: 4/2019. számú iránymutatás a 25. cikk szerinti beépített és alapértelmezett adatvédelemről 2.0 változat. Elfogadás időpontja: 2020. október 20.

EDPB: 5/2019. számú vélemény az elektronikus hírközlési adatvédelmi irányelv és az általános adatvédelmi rendelet közötti kölcsönhatásról, különösen az adatvédelmi hatóságok illetékessége, feladatai és hatásköre tekintetében. Az elfogadás időpontja: 2019. március 12.

EDPB: 5/2020 Iránymutatás az (EU) 2016/679 rendelet szerinti hozzájárulásról 1.1 verzió. Elfogadás időpontja: 2020. május 4.

EDPB: 8/2020. sz. iránymutatás a közösségi média felhasználóinak megcélzásáról. 2.0. változat. Elfogadás időpontja: 2021. április 13.

EDPB: 'Safeguarding individuals' digital rights: EDPB Annual Report 2023. 2024. április 23. [edpb_annual_report_2023_en.pdf](#) (letöltés: 2024. 05. 23.)

EDPB: Contribution of the EDPB to the report on the application of the GDPR under Article 97 Adopted on 12 December 2023. https://www.edpb.europa.eu/system/files/2023-12/edpb_contributiongdprevaluation_20231212_en.pdf (letöltés: 2024. 08. 22.)

P9_TA(2021)0256. European Parliament: 2019-2024:Texts Adopted. https://www.europarl.europa.eu/doceo/document/TA-9-2021-0256_EN.pdf (letöltés: 2025. 01. 03.)

Európai uniós dokumentumok

2009/C 45/02. A Bizottság közleménye – Iránymutatás az EK-Szerződés 82. cikkének az erőfölényben lévő vállalkozások versenykorlátozó visszaélő magatartására történő alkalmazásával kapcsolatos bizottsági jogérvényesítési prioritásokról

2010/C 280/01. Az európai adatvédelmi biztos véleménye az információs társadalom iránti bizalomnak az adatok és a magánélet védelme elősegítése révén történő erősítéséről

2014/C 225/07. Az európai adatvédelmi biztos előzetes véleményének összefoglalója az adatvédelemről és a versenyképességről az óriás méretű adathalmazok korában

2017/0003/COD eljárás lépései. <https://eur-lex.europa.eu/legal-content/HU/HIS/?uri=CELEX:52017PC0010> (letöltés: 2024. 12. 20.)

2021/C 525/01. A Bizottság közleménye a fogyasztók jogairól szóló 2011/83/EU európai parlamenti és tanácsi irányelv értelmezésére és alkalmazására vonatkozó iránymutatásról

2021/C 526/01. A Bizottság közleménye – Iránymutatás a belső piacon az üzleti vállalkozások fogyasztókkal szemben folytatott tisztességtelen kereskedelmi gyakorlatairól szóló 2005/29/EK európai parlamenti és tanácsi irányelv értelmezéséhez és alkalmazásához

COM(2015) 192 végleges. A Bizottság közleménye az Európai Parlamentnek, a Tanácsnak, az Európai Gazdasági és Szociális Bizottságnak és a Régiók Bizottságának: Európai digitális egységes piaci stratégia. Brüsszel, 2015. 05. 06.

COM(2016) 288 final. A Bizottság közleménye az Európai Parlamentnek, a Tanácsnak, az Európai Gazdasági és Szociális Bizottságnak és a Régiók Bizottságának: Online platformok és a digitális egységes piac: Lehetőség és kihívás Európa számára. Brüsszel, 2016. 05. 25.

COM(2016) 587 végleges. A Bizottság közleménye az Európai Parlamentnek, a Tanácsnak, az Európai Gazdasági és Szociális Bizottságnak és a Régiók Bizottságának: Az összekapcsoltság a versenyképes digitális egységes piaci szolgáltatásban: Úton a gigabitalapú európai információs társadalom felé. Brüsszel, 2016. 09. 14.

COM(2017) 10 final. Javaslat. Az Európai Parlament és a Tanács rendelete az elektronikus hírközlés során a magánélet tiszteletben tartásáról és a személyes adatok védelméről, valamint a 2002/58/EK irányelv hatályon kívül helyezéséről (elektronikus hírközlési adatvédelmi rendelet). Brüsszel, 2017. 01. 10.

COM(2018) 183 final. A Bizottság közleménye az Európai Parlamentnek, a Tanácsnak és az Európai Gazdasági és Szociális Bizottságnak: Új megállapodás a fogyasztói érdekekért. Brüsszel, 2018. 04. 11.

COM(2020) 264 final. A Bizottság közleménye az Európai Parlamentnek és a Tanácsnak: A polgárok szerepe erősítésének és az EU digitális átállással kapcsolatos megközelítésének pillérét képező adatvédelem – az általános adatvédelmi rendelet alkalmazásának két éve. Brüsszel, 2020. 06. 24.

COM(2021) 713 final. A Bizottság közleménye az Európai Parlamentnek, a Tanácsnak, az Európai Gazdasági és Szociális Bizottságnak és a Régiók Bizottságának: Az új kihívásokra felkészült versenypolitika. Brüsszel, 2021. 11. 18.

COM(2022) 212 final. A Bizottság közleménye az Európai Parlamentnek, a Tanácsnak, az Európai Gazdasági és Szociális Bizottságnak és a Régiók Bizottságának: Digitális évtized a gyermekek és az ifjúság számára: a gyermekbarát internetre (BIK+) vonatkozó új európai stratégia. Brüsszel, 2022. 05. 11.

COM(2024) 258 final. A Bizottság jelentése az Európai Parlamentnek és a Tanácsnak a 93/13/EGK tanácsi irányelvnek, valamint a 98/6/EK, a 2005/29/EK és a 2011/83/EU európai parlamenti és tanácsi irányelvnek az uniós fogyasztóvédelmi szabályok hatékonyabb végrehajtása és korszerűsítése tekintetében történő módosításáról szóló, 2019. november 27-i (EU) 2019/2161 európai parlamenti és tanácsi irányelv végrehajtásáról. Brüsszel, 2024. 06. 18.

COM(2024) 357 final. A Bizottság közleménye az Európai Parlamentnek és a Tanácsnak: Második jelentés az általános adatvédelmi rendelet alkalmazásáról. Brüsszel, 2024. 07. 25.

COM(2025) 45 final. Annexes 1 to 5. Annexes to the Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions. Commission work programme 2025. Strasbourg, 2025. 02. 11.

COM(2025) 47 final. A Bizottság közleménye az Európai Parlamentnek, a Tanácsnak, az Európai Gazdasági és Szociális Bizottságnak és a Régiók Bizottságának: Egyszerűbb és gyorsabb Európa: Közlemény a végrehajtásról és az egyszerűsítésről. Strasbourg, 2025. 02. 11.

COM(2025) 837 final. Javaslat. Az Európai Parlament és a Tanács rendelete az (EU) 2016/679, az (EU) 2018/1724, az (EU) 2018/1725 és az (EU) 2023/2854 rendelet, valamint a 2002/58/EK, az (EU) 2022/2555 és az (EU) 2022/2557 irányelv digitális jogszabályi keret egyszerűsítése tekintetében történő módosításáról, valamint az (EU) 2018/1807, az (EU) 2019/1150 és az (EU) 2022/868 rendelet és az (EU) 2019/1024 irányelv hatályon kívül helyezéséről. Brüsszel, 2024. 11. 19.

NOYB.EU: *Digital Omnibus Analysis of Select GDPR and ePrivacy Proposals by the European Commission Version 2.0.* 2026. január. <https://noyb.eu/sites/default/files/2025-12/noyb%20Digital%20Omnibus%20Report%20V1.pdf>. (letöltés: 2026. 02. 01.)

PE 690.619. Nikolina ŠAJN: *Briefing EPRS (European Parliamentary Research Service): Vulnerable consumers*, 2021. május

ST 6087 2021 INIT. Proposal for a Regulation of the European Parliament and of the Council concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications)

SWD(2017) 4 final. Bizottsági szolgálati munkadokumentum: a hatásvizsgálat vezetői összefoglalója, amely a következő dokumentumot kíséri: Javaslat – Az Európai Parlament és a Tanács rendelete az elektronikus hírközlés során a magánélet tiszteletben tartásáról és a személyes adatok védelméről, valamint a 2002/58/EK irányelv hatályon kívül helyezéséről (elektronikus hírközlési adatvédelmi rendelet). Brüsszel, 2017. 01. 10.

SWD(2024) 230 final. European Commission: *Commission staff working document fitness check of EU consumer law on digital fairness*. Brüsszel, 2024. 10. 03.

Edps.europa.eu: Big Data & Digital Clearinghouse. [Big Data & Digital Clearinghouse | European Data Protection Supervisor](#) (letöltés: 2024. 10. 20.)

European Data Protection Supervisor: Opinion 4/2017 on the Proposal for a Directive on certain aspects concerning contracts for the supply of digital content

European Commission: Behavioural study on unfair commercial practices in the digital environment: dark patterns and manipulative personalisation. Final Report. 2022. <https://data.europa.eu/doi/10.2838/859030> (letöltés: 2023. 06. 01.),

European Commission: Special group on the EU Code of conduct on age-appropriate design. 2023. 09. 20. <https://digital-strategy.ec.europa.eu/en/policies/group-age-appropriate-design> (letöltés: 2024. 08. 04.)

European Commission: Adequacy decisions. https://commission.europa.eu/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en?prefLang=hu (letöltés: 2024. 12. 22.)

European Commission – EDPB: Joint Guidelines on the Interplay between the Digital Markets Act and the General Data Protection Regulation. 2025. 10. 09. https://www.edpb.europa.eu/our-work-tools/documents/public-consultations/2025/joint-guidelines-interplay-between-digital_hu (letöltés: 2025. 11. 12.)

Egyéb irodalom

AGCM: Facebook fined 10 million Euros by the ICA for unfair commercial practices for using its subscribers' data for commercial purposes. Sajtóközlemény, 2018. 12. 07. [AGCM - Autorita' Garante della Concorrenza e del Mercato](#) (letöltés: 2024. 02. 02.)

ARNOW, Grant: Apple watch-ing you: Why wearable technology should be federally regulated. <https://digitalcommons.lmu.edu/cgi/viewcontent.cgi?article=2973&context=llr> (letöltés: 2018. 11. 23.)

BOLCSÓ Dániel: *Évtizedes vita ért véget: az Apple-nek gigantikus adóhátralékot kell fizetnie az EU-ban.* 2024. szeptember 10. <https://telex.hu/gazdasag/2024/09/10/apple-europai-unio-birosaga-13-milliard-euro-birsag-adozas-irorszag> (letöltés: 2024. 10. 02.)

Bundeskartellamt: Facebook proceeding concluded. Sajtóközlemény, 2024. 10. 10. https://www.bundeskartellamt.de/SharedDocs/Meldung/EN/Pressemitteilungen/2024/10_10_2024_Facebook.html (letöltés: 2025. 01. 10.)

BURGESS, Matt: *How GDPR Is Failing.* <https://www.wired.com/story/gdpr-2022/> (letöltés: 2023. 03. 03.)

Cookiepedia by OneTrust. <https://cookiepedia.co.uk/> (megtekintés: 2024. 10. 22.)

DATA PROTECTION COMMISSION: *Annual Report* 2023. https://www.dataprotection.ie/sites/default/files/uploads/2024-05/DPC%20EN_AR%202023_Final%20.pdf (letöltés: 2025. 12. 03.)

DATA PROTECTION COMMISSION: *Annual Report* 2024. https://www.dataprotection.ie/sites/default/files/uploads/2025-06/DPC_Annual_Report_EN_Low_Res.pdf (letöltés: 2025. 12. 03.)

EHANGZHOU.GOV.CN: *Digital economy becomes new growth engine for China and other G20 members.* 2024. augusztus 6. https://www.ehangzhou.gov.cn/2024-08/06/c_282384.htm (letöltés: 2024. 11. 05.)

EC.EUROPA.EU: *Commission clears acquisition of Fitbit by Google, subject to conditions.* Sajtóközlemény, 2020. december 17. [Mergers: Commission clears acquisition of Fitbit by Google \(europa.eu\)](#) (letöltés: 2022. 11. 10.)

EDPB.EUROPA.EU: *Az általános adatvédelmi rendelet célzott módosításai: EDPB & az európai adatvédelmi biztos üdvözli a nyilvántartási kötelezettségek egyszerűsítését, és további pontosítást kér.* Sajtóközlemény, Brüsszel, 2025. július 9. https://www.edpb.europa.eu/news/news/2025/targeted-modifications-gdpr-edpb-edps-welcome-simplification-record-keeping_hu (letöltés: 2025. 10. 12.)

EUCONSENT.EU: *euCONSENT announces the AgeAware App – device-based online age assurance.* Sajtóközlemény, 2024. április 12. <https://euconsent.eu/euconsent-announces-the-ageaware-app-device-based-online-age-assurance/> (letöltés: 2024. 05. 12.)

EUROPA.EU: *A személyes adatok védelme, internetes adatvédelem* (2021). https://europa.eu/youreurope/citizens/consumers/internet-telecoms/data-protection-online-privacy/index_hu.htm. (letöltés: 2021. 04. 22.)

EURÓPAI BIZOTTSÁG: *A Bizottság uniós adatvédelmi reformjáról született megállapodás felfoldja a digitális egységes piacot.* Sajtóközlemény, Brüsszel, 2015. december 15. http://europa.eu/rapid/press-release_IP-15-6321_hu.htm (letöltés: 2018. 11. 28.)

EURÓPAI BIZOTTSÁG: *A Bizottság megállapítja, hogy az Apple és a Meta megsértette a digitális piacokról szóló jogszabályt.* Sajtóközlemény, Brüsszel, 2025. 04. 23. https://ec.europa.eu/commission/presscorner/detail/hu/ip_25_1085 (letöltés: 2025. 11. 05.)

EURÓPAI BIZOTTSÁG: *Adatvédelem: az Európai Bizottság az EU és az USA közötti biztonságos és megbízható adatáramlásra vonatkozó új megfelelőségi határozatot fogadott el.* Sajtóközlemény, Brüsszel, 2023. július 10. https://ec.europa.eu/commission/presscorner/api/files/document/print/hu/ip_23_3721/IP_23_3721_HU.pdf (letöltés: 2024. 12. 12.).

GALÁNTAI Zoltán: *E-privacy olvasókönyv. Dialógusok a privacyről és az internetről – meg a cyberpornóról, a megfigyelésekről és egyebekről.* <https://mek.oszk.hu/04100/04134/html/#7> (letöltés: 2022. 03. 06.)

GDPRBIRSAGOK.HU: *GDPR bírságok.* [GDPR bírságok Magyarországon](#) (letöltés: 2023. 03. 06.)

GVH: *Összehangolt európai fellépés a Temu-val szemben.* Sajtóközlemény, 2024. 11. 08. [Összehangolt európai fellépés a Temu-val szemben - GVH](#) (letöltés: 2024. 12. 10.)

HABÓK Lilla: *Cambridge Analytica: miről szól a Facebook-botrány?* <https://www.hwsz.hu/hirek/58575/facebook-scl-cambridge-analytica-pszichografikus-profilozas.html> (letöltés: 2018. 11. 24.)

HRECSKA Renáta: *Fogyasztói döntéshozatali folyamat az információs közgazdaságtan és a viselkedési gazdaságtan eredményeinek tükrében,* 2012. http://www.gvh.hu/data/cms1000468/Hrechka_Ren%C3%A1ta_tanulm%C3%A1ny.pdf (letöltés: 2019. 06. 02.)

KOI Tamás: *Írország elfogadja a globális minimumadót.* Hír, 2021. október 8. <https://www.hwsz.hu/hirek/63844/irorszag-g20-oecd-tarsasagi-ado.html> (letöltés: 2024. 10. 02.)

KOLTAY Gábor – VINCZE János: *Fogyasztói döntések a viselkedési közgazdaságtan szemszögéből.* Közgazdasági Szemle 2009/6. 495–525.

KOZMA Zoltán – ALMÁSY Márk: *Közel 6 milliárd euró bírság a GDPR óta.* Blogbejegyzés 2025. 01. 29. <https://blogs.dlapiper.com/advocatus/2025/01/kozel-6-milliard-euro-birsag-a-gdpr-ota/> (letöltés: 2025. 02. 13.)

LOVAS Gergő: *A brit nagykövethelyettes a koronavírus egyik áldozata Magyarországon.* Index.hu, 2020. március 25. <https://bit.ly/3qqUzwo> (letöltés: 2021. 03. 03.)

MADRIGAL, Alexis C.: *Reading the Privacy Policies You Encounter in a Year Would Take 76 Work Days.* 2012. március 1. [Reading the Privacy Policies You Encounter in a Year Would Take 76 Work Days - The Atlantic](#) (letöltés: 2020. 01. 02.)

ONLINEPLATFORMOK.HU: *Célkeresztben a TikTok: Bizottsági vizsgálatok.* 2024. április 30. <https://onlineplatformok.hu/cikk/celkeresztben-a-tiktok-bizottsagi-vizsgalatok> (megtekintés: 2024. 05. 30.)

TAMIM, James: *What is the EU Digital Fairness Act (DFA)?* 2025. 12. 09. <https://digitalfairnessact.com/what-is-the-digital-fairness-act> (letöltés: 2025. 12. 30.)

TAMIM, James: *Will the Digital Fairness Act be a Regulation?* Hír, 2024. 12. 09. <https://digitalfairnessact.com/will-the-digital-fairness-act-be-a-regulation> (letöltés: 2025. 03. 02.)

The future of European competitiveness Part A: A competitiveness strategy for Europe. 2024. szeptember. https://commission.europa.eu/topics/competitiveness/draghi-report_en (letöltés: 2025. 11. 05.)

The future of European competitiveness Part B: In-depth analysis and recommendations. 2024. szeptember. https://commission.europa.eu/topics/competitiveness/draghi-report_en (letöltés: 2025. 11. 05.)

TÓTH Krisztina: *Mi lesz veled direkt marketing?* https://jogaszvilag.hu/uzlet/mi-lesz-veled-direkt-marketing/#_ftn1 (letöltés: 2019. 06. 02.)