DOI: 10.59851/imr.12.2.3 IN MEDIAS RES 2023/2. • 3, 45–68

A GDPR és a Digital Markets Act viszonyának tisztázása

TÓTH ANDRÁS – SZABÓ ENDRE GYŐZŐ – NÉMETH SZABOLCS – RUDICS REGINA – RIDEG GERGELY*

A Digital Markets Act az európai uniós jogalkotásnak a meglévő uniós joganyagra, többek között az általános adatvédelmi rendeletre is szervesen épülő újdonsága, amely a techóriások célzott regulációját kívánja megvalósítani. Míg korábban az uniós szabályozás sarokkövének számított a személyes adatok és a magánszféra alapjogi szintű védelme, addig mára szintén prioritássá vált az Európai Unió számára az adatalapú gazdaság lehetőségeinek kiaknázása, az európai piacok versenyképességének növelése. A tanulmányban a digitális piacokról szóló jogszabály, a digitális szolgáltatásokról szóló rendelet és az általános adatvédelmi rendelet azon pontjaira mutatunk rá, amelyek kapcsolata a jövőben meghatározó lesz a versenyképes és adatközpontú európai gazdaság kialakítása szempontjából. Vizsgáljuk az általános adatvédelmi rendelet elsődlegességét, esetleges lex specialis jellegét, továbbá a digitális piacokról szóló jogszabály által bevezetett tilalmakat, például az üzleti felhasználók és/vagy a fogyasztók adatainak saját célra való felhasználásának tilalmát és a platform különböző szolgáltatásaiból származó felhasználói adatok kombinálásának tilalmát. Végezetül kitérünk a digitális piacokról szóló jogszabály és az európai adatvagyon megőrzésének kapcsolataira.

Kulcsszavak: DMA, GDPR, adatvédelem, digitalizáció, adathordozhatóság

A Clarification of the Relationship Between GDPR and DMA

The Digital Markets Act is a new piece of EU legislation that builds on existing EU legislation, including the General Data Protection Regulation, to target regulation of tech giants. While the protection of personal data and privacy at a fundamental rights level used to be the cornerstone of EU regulation, the EU has now also made it a priority to exploit the benefits of a data-driven economy and to increase the competitiveness of European markets. In this paper, we highlight the points of the Digital Markets Act, Digital Services Actand General Data Protection Regulation whose interplay will be crucial for the future development of a competitive and data-driven European economy. We will examine the primacy of the General Data Protection Regulation, its possible lex specialis nature, and the prohibitions introduced by the Digital Markets Act, such as the prohibition to use business users' and/or own consumers' data for private purposes, or the prohibition to combine user data from different services of the platform. Finally, we will discuss the relationship between the Digital Markets Act and the preservation of the European data assets.

Keywords: DMA, GDPR, data protection, digitalization, data portability

* Tóth András: habilitált egyetemi docens, Károli Gáspár Református Egyetem Állam- és Jogtudományi Kar.
Szabó Endre Győző: adatvédelmi szakértő, a Nemzeti Adatvédelmi és Információszabadság Hatóság korábbi elnökhelyettese (2012–2023 között).
Németh Szabolcs: adatvédelmi felelős, Nemzeti Filmintézet.
Rudics Regina: PhD-hallgató, Károli Gáspár Református Egyetem Állam- és Jogtudományi Kar.
Rideg Gergely: PhD-hallgató, Károli Gáspár Református Egyetem Állam- és Jogtudományi Kar.

1. A DMA-nak a GDPR szempontjából releváns rendelkezései

A nagy online platformok közvetítőként működnek az üzleti felhasználók vagy reklámozók és a végfelhasználók között. Egyesek közvetlenül is versenyeznek az üzleti felhasználókkal azáltal, hogy saját termékeiket és szolgáltatásaikat kínálják, az alapvető termékkínálatukba integrálva.[1] A részletes fogyasztói profilalkotással összefüggő átláthatósági kötelezettségek segítik az Európai Unió általános adatvédelmi rendeletének (GDPR)[2] végrehajtásával összefüggő információszolgáltatást, míg az adatok alapvető platformszolgáltatások közötti kombinálásának szabályozása kiegészíti a GDPR nyújtotta védelem már meglévő szintjét. A digitális piacokról szóló jogszabály (DMA)[3] pontosítja, hogy a kapuőrök feladata biztosítani, hogy a rendeletben megállapított kötelezettségeknek való megfelelés az egyéb jogok, érdekek – például a személyes adatok és a magánélet vagy a fogyasztók –védelmét szolgáló uniós jogszabályokkal való teljes összhang mellett valósuljon meg.

A kapuőrök alapvető platformszolgáltatást nyújtó vállalkozások, e szolgáltatások körét a DMA rögzíti.[4] A feltételeknek megfelelő vállalkozást a DMA 3. cikkében meghatározott eljárás szerint az Európai Bizottság minősíti kapuőrré. A piac monopolisztikus irányba eltorzult jellegét és a szabályozás igényét mutatja, hogy korábban példa nélküli koncentráció jött létre a kommunikációs piacon. Az online keresőszolgáltatások terén 80 százalékos, míg a közösségi média területén 70 százalékos részesedéssel bír a piacvezető vállalkozás.[5] A DMA az európai uniós jogalkotásnak a már meglévő uniós joganyagra, így többek között a GDPR-ra is épülő újdonsága. Erre lehet következtetni a preambulumbekezdések koherens és rendszerezett szóhasználatából is. Habár, mint említettük, a DMA alapvetően újfajta trösztellenes szabályozás, amely az Európai Unió működéséről szóló szerződés (EUMSZ) 114. cikkére történő hivatkozásával elhelyezi magát mint irányultságát tekintve nem kizárólag versenyvédelmi, de a digitális belső piacnyitásért is felelős szabályozást,[6] azt is fontos kiemelni, hogy a GDPR szempontjából számos releváns rendelkezést tartalmaz. A következőkben – a teljesség igénye nélkül – ezeket a főbb rendelkezéseket tesszük vizsgálatunk tárgyává.

---

1 Christophe Carugati: How to implement the self-preferencing ban in the European Union's Digital Markets Act. *Bruegel,* 2022. december 2., https://bit.ly/47LjRct.

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 rendelet hatályon kívül helyezéséről (általános adatvédelmi rendelet) (GDPR).

3 Az Európai Parlament és a Tanács (EU) 2022/1925 rendelete a digitális ágazat vonatkozásában a versengő és tisztességes piacokról, valamint az (EU) 2019/1937 és az (EU) 2020/1828 irányelv módosításáról (digitális piacokról szóló jogszabály) (Digital Markets Act, DMA).

4 A DMA 2. cikk (2) bekezdése szerint alapvető platformszolgáltatás az online közvetítő szolgáltatás, az online keresőprogram, az online közösségi hálózati szolgáltatás, a videómegosztóplatform-szolgáltatás, a számfüggetlen személyközi hírközlési szolgáltatás, az operációs rendszer, a webböngésző, a virtuális asszisztens, a felhőszolgáltatás, valamint az online hirdetési szolgáltatás. A feltételeknek megfelelő vállalkozást a DMA 3. cikkében meghatározott eljárás szerint az Európai Bizottság minősíti kapuőrré.

5 Annegret Bendiek: Integrationspolitische Bedeutung des Digital Service Act (DSA) und Digital Markets Act (DMA). *Stiftung Wissenschaft und Politik,* 2021. március 1., https://bit.ly/47Mc3HC, 3.

6 Andreas Heinemann – Giulia M. Meier: Der Digital Markets Act (DMA): Neues „Plattformrecht" für mehr Wettbewerb in der digitalen Wirtschaft. *Zeitschrift für Europarecht,* 2021, 86–101.

Az európai adatvédelmi politika szempontjából az sejthető, hogy a platformok szabályozása a digitális szolgáltatásokról szóló rendelet (DSA)[7] és a DMA rendelkezései és azok betartása, betartatása révén az algoritmusok nagyobb átláthatóságához fog vezetni.[8] A magasabb fokú transzparencia az adatvédelem erősödését eredményezi, ami az EU adatstratégiájának is egyik fő célkitűzése.[9] Azt kell gondoljuk, hogy a DSA-t és a DMA-t mint jogalkotási csomagot együtt kell értelmezni, és hogy azok célja a nagyméretű adatok, valamint a mesterséges intelligencia mobilizálása és regulázása, továbbá a GDPR önmagában nem képes az ezekkel kapcsolatos minden adatvédelmi kérdést kezelni.[10]

1.1. Alapfogalmak

A DMA 2. cikkében mindösszesen 33 fogalmat határoz meg, amelyek közül hármat (személyes adat, profilalkotás és hozzájárulás) a GDPR meghatározására visszautalva használ. A személyes adat így a DMA rendelkezéseiben is a GDPR 4. cikk 1. pontjában meghatározott személyes adat.[11] Megemlítendő ugyanakkor, hogy a GDPR tekintetében az alapegység a „személyes adat", míg a DMA-ban az „adat": ilyenek lehetnek „aktusok, tények vagy információk bármilyen digitális megjelenítései, vagy az ilyen aktusok, tények és információk összeállításai, ideértve a hang-, kép- vagy audiovizuális felvétel formájában történő megjelenítést is". A DMA tehát tágabb kört von az adat fogalma alá, ami a szabályozás hatályával is magyarázható. Míg a GDPR a természetes személyek magánszféráját hivatott védeni, addig a DMA a belső piac megfelelő működéséhez szükséges szabályokat rögzíti, és e tekintetben nem elsődleges szempont, hogy az adat összefüggésbe hozható-e természetes személlyel vagy sem.[12]

1.2. Az üzleti felhasználók és a saját fogyasztók adatainak saját célra történő felhasználásának tilalma

A DMA 6. cikk (2) bekezdése speciális tilalmat állít fel a kapuőrök számára, nevezetesen az üzleti felhasználók és/vagy a saját fogyasztók adatainak saját célra való felhasználásának tilalmát.

---

7 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 (digitális szolgáltatásokról szóló rendelet) (Digital Services Act, DSA).

8 Ulrich Kelber: EU-Digitalstrategie und die dazugehörigen Rechtsakte von DGA, DMA, DSA und AIA – Auswirkungen für den Datenschutz. *Bundesbeauftragten für den Datenschutz und die Informationsfreiheit,* 2022. január 27., https://bit.ly/47O22cH.

9 Európai adatstratégia. A Bizottság közleménye az Európai Parlamentnek, a Tanácsnak, az Európai Gazdasági és Szociális Bizottságnak és a Régiók Bizottságának, https://bit.ly/49Q40et, 6.

10 Kelber i. m. (8. lj.).

11 „Személyes adat": azonosított vagy azonosítható természetes személyre („érintett") 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.

12 A DMA nemcsak a személyes, hanem a nem személyes adat fogalmát is meghatározza a 2. cikk (26) bekezdésében.

A tilalom szempontjából az alább idézett 5. cikk (2) bekezdés c) pontja és a 6. cikk (2) bekezdése együtt is értelmezendő. Ennek eredményeként a DMA kimondja, hogy a kapuőr minden platform vonatkozásában tartózkodik attól, hogy az üzleti felhasználókkal való verseny során felhasználja azokat a nyilvánosan nem elérhető adatokat,[13] amelyek az alapvető platformszolgáltatás üzleti felhasználóinak tevékenységein keresztül keletkeznek, beleértve a szóban forgó üzleti felhasználók végfelhasználóit, vagy amelyeket a platformszolgáltatásainak az üzleti felhasználói vagy ezen üzleti felhasználók végfelhasználói adtak meg. A kapuőrök nem korlátozhatják a végfelhasználók szabad választását oly módon, hogy technikailag megakadályozzák a különböző szoftveralkalmazások és szolgáltatások közötti váltást vagy az azokra történő előfizetést. Tehát a szabad választást attól függetlenül biztosítani kell, hogy ők gyártják-e azt a hardvert, amellyel e szoftveralkalmazások vagy a szolgáltatások hozzáférhetők. Nem támaszthatnak mesterséges technikai akadályokat, hogy a váltást ellehetetlenítsék vagy eredménytelenné tegyék.

A végfelhasználóknak is szabad kezet kell kapniuk abban, hogy válasszanak ezen üzleti felhasználók kínálatából, szerződést kössenek velük, akár a kapuőr által nyújtott alapvető platformszolgáltatás révén, az üzleti felhasználó közvetlen értékesítési csatornáján keresztül, akár a szóban forgó üzleti felhasználó által használt egyéb közvetett módon. Ez vonatkozik az ajánlatok promóciójára és az üzleti felhasználók és a végfelhasználók közötti szerződéskötésre is. Emellett nem ásható alá és nem korlátozható a végfelhasználók azon képessége sem, hogy szabadon vásároljanak tartalmat, előfizetést, funkciókat vagy egyéb tételeket a kapuőr által nyújtott alapvető platformszolgáltatáson kívül. Különösen azt kell elkerülni, hogy a kapuőrök az alapvető platformszolgáltatásukon futó szoftveralkalmazás segítségével korlátozzák a végfelhasználókat abban, hogy az ilyen szolgáltatásokhoz hozzáférjenek és igénybe vegyék azokat. Például egy szoftveralkalmazás-letöltésen kívül vásárolt vagy szoftveralkalmazás-áruházból vásárolt online tartalom előfizetőit nem szabad megakadályozni abban, hogy ehhez a tartalomhoz a kapuőr alapvető platformszolgáltatásán futó szoftveralkalmazáson keresztül férjenek hozzá csak azért, mert azt e szoftveralkalmazáson vagy szoftveralkalmazás-áruházon kívül vásárolták.[14] E tilalmakkal kapcsolatban is az a jogalkotó célja, hogy minél inkább megelőzze a platform korlátozó magatartását, amelyet az a kettős szerepét kihasználva képes gyakorolni. A tilalomhoz kapcsolódik az 5. cikk (2) bekezdésében foglalt rendelkezés, amely szerint „a kapuőr c) a releváns alapvető platformszolgáltatásokból származó személyes adatokat nem használhatja fel általa külön nyújtott egyéb szolgáltatások – például egyéb alapvető platformszolgáltatások – céljára, és fordítva". Az EU a nagy platformszolgáltatókkal vívott csatában gyűjtött tapasztalatait is felhasználva alkotta meg ezt a tilalmat. Az egyik ilyen eset volt az Európai Bizottság által az Amazon ellen 2020 novemberében indított eljárás. Az Amazonhoz hasonló platformoknak ugyanis előnyük van kettős szerepükből adódóan: egyrészt mint piaci szolgáltató, másrészt mint eladó is fellépnek. „Az Amazon összegyűjti a felhasználói adatokat, például a vásárlói preferenciákat, és ezeket az adatokat arra használja fel, hogy saját termékeinek értékesítését optimalizálja. Ezen túlmenően az Amazon hirdetheti saját termékeit, míg a versenytársak termékei háttérbe szorulnak."[15]

13 DMA 6. cikk (2) bekezdés.

14 DMA (40) preambulumbekezdés.

15 Verfahren gegen US-Konzern. EU wirft Amazon Kartellverstöße vor. *Tagesschau,* 2020. november 10, https://bit.

1.3. A platform sokszínűségéből származó felhasználói adatok helyzete – a platform különböző szolgáltatásaiból származó felhasználói adatok kombinálásának tilalma

A kapuőrök általában kettős funkciót töltenek be: egyszerre alapvető platformszolgáltatók és versenyzők. Ez utóbbi mivoltukban versenghetnek az ugyanazon végfelhasználók részére nyújtott szolgáltatás vagy termék értékesítése terén, ami abból a szempontból aggályos, hogy az üzleti felhasználóik által gyűjtött adatokat – amelyeket az alapvető platformon folytatott ügyletekből nyertek – a saját szolgáltatásaik céljára használják fel, miközben az üzleti felhasználóhoz hasonló szolgáltatást nyújtanak. Annak megakadályozására, hogy a kapuőrök tisztességtelen módon hasznot húzzanak kettős szerepükből, biztosítani kell, hogy tartózkodjanak bármely olyan összesített vagy nem összesített adat (melyek közt nyilvánosan nem elérhető anonimizált[16] és személyes adatok is lehetnek) olyan módon való felhasználásától, hogy az üzleti felhasználóik szolgáltatásaihoz hasonló szolgáltatásokat kínáljanak. Ez a kötelezettség arra az üzletágra vonatkozik, amelyik az alapvető platformszolgáltatás üzleti felhasználóival versenyez.[17]

Előfordulhat, hogy a kapuőr hirdetési szolgáltatást is nyújtó alapplatformként funkcionál. Ilyenkor az üzleti felhasználók hirdetési szolgáltatást vesznek a platformtól, és így megesik, hogy az adatok nem az alapvető platformszolgáltatásban keletkeznek, hanem azokat az üzleti felhasználó adja meg az alapvető platformszolgáltatásnak vagy annak műveletei alapján az érintett alapvető platformszolgáltatáson keresztül keletkeznek. Ezt a problémát felismerve a DMA korlátozásokat vezet be, amelyeket lentebb részletezünk.[18] Ha a platform hirdetési szolgáltatása megfelel az egyenlő bánásmód előírásának, akkor természetesen nem ütközik a DMA-ba. Az adatok alapvető platformszolgáltatások közötti kombinálásának tilalma kiegészíti a GDPR által biztosított védelmet.

A DMA 5. cikke részletes szabályokat állapít meg a személyes adatok kezelésére vonatkozóan. Ezeket a szabályokat tilalomként fogalmazta meg a jogalkotó. Míg a személyes adatok kezelésére vonatkozó szabályok általában a megengedett magatartásokat határozzák meg, itt a DMA részletez bizonyos üzleti gyakorlatokat, amelyek olyannyira tisztességtelenek, hogy azokat az uniós jogalkotó tiltani lát szükségesnek. Ezeknek a tilalmaknak az elemzése annak bemutatására is szolgál, hogy milyen mértékben és milyen kizsákmányoló jelleggel használják a platformok a különböző módokon birtokukba jutó személyes adatokat.

A DMA előírja a kapuőrnek, hogy az üzleti felhasználói ügyfeleire vonatkozó adatait nem kezelheti online hirdetési szolgáltatások nyújtása céljából – tehát azokat az adatokat, amelyek birtokába nem a saját közreműködése, üzleti teljesítménye révén jut, nem használhatja fel saját

ly/3sLqL2z; Hendrik Zimmermann – Caroline Heinzel: Der Digital Markets Act. Plattform-Regulierung für Demokratie und Nachhaltigkeit in der EU–aktueller Stand und Verbesserungspotenziale, *Germanwatch,* 2022. január, https://bit.ly/3GaQogo.

16 GDPR (26) preambulumbekezdés: „Az adatvédelem elveit ennek megfelelően az anonim információkra nem kell alkalmazni, nevezetesen olyan információkra, amelyek nem azonosított vagy azonosítható természetes személyre vonatkoznak, valamint az olyan személyes adatokra, amelyeket olyan módon anonimizáltak, amelynek következtében az érintett nem vagy többé nem azonosítható."

17 DMA (46) preambulumbekezdés.

18 DMA (47) preambulumbekezdés.

hirdetési céljára.[19] Helyesnek tartjuk ezt a szabályozói megoldást; úgy is fogalmazhatunk, hogy a DMA ezzel az adatok tisztességtelen kizsákmányolásának az egyik lehetőségét tiltja meg.

A következő tilalom szerint a kapuőr nem kapcsolhatja össze, nem kombinálhatja az alapvető platformszolgáltatásból származó személyes adatokat más szolgáltatásból származó adatokkal – itt a DMA gyakorlatilag a rendelkezésre álló adatállomány felszeletelését írja elő.[20] A tilalom vonatkozik a platform- vagy más szolgáltatásból és a harmadik fél által nyújtott szolgáltatásból származó adatokra is. Ha úgy tetszik, az egyes szolgáltatásokat külön célként definiálja, és ilyen módon a célhoz kötött adatkezelés elvét alkalmazza a legnagyobb szolgáltatásokra és szab korlátot annak, hogy az egyik célból gyűjtött adatokat aztán egy másik célra korlátozás nélkül felhasználják. A cél az adatvédelmi és versenyjogi szempontból is értékelhető, túlzott adatösszekapcsolások megakadályozása. Ugyanis a különböző forrásokból származó végfelhasználói adatok kombinációja a kapuőrök különböző szolgáltatásaiban potenciális előnyöket biztosít a kapuőröknek az adatfelhalmozás tekintetében, ami viszont a piacra lépés akadályait erősíti.[21]

A DMA 5. cikkében meghatározott harmadik tilalom szerint a kapuőr az alapvető platformszolgáltatásból származó személyes adatokat nem használhatja fel egyéb szolgáltatások céljára – sem fordítva. A jogszabály angol verziója a cross-use kifejezést használja, amelyet a magyar fordítás nem ad tisztán vissza.[22] Itt is a túlzott adatkoncentráció ellenében hat a szabályozás, és a kapuőr rendelkezésére álló számos, a magánszférát jelentősen érintő összekapcsolás lehetőségét szorítja jogi korlátok közé.

A tilalmak sorát az a rendelkezés zárja, amely szerint a kapuőr a végfelhasználókat nem léptetheti be más szolgáltatásba, hogy a személyes adatokat összekapcsolja.[23] Ennél a pontnál is arra kell felhívnunk a figyelmet, hogy tilalom hiányában ez a platformok általános gyakorlata volt, és ennek sem jogi, sem technikai, sem üzleti akadály nem állt az útjába. A DMA mindezen tilalmak esetében közvetlenül avatkozik be olyan viszonyokba, amelyeknél korábban a kapuőrön kívül mások nem voltak tárgyalási pozícióban. A monopolisztikus piac adatvédelmi jogi kiigazításáról van itt szó, amely bár a GDPR-t kifejezetten nem hívja fel, de annak eszközrendszerét alkalmazza a szabályozott ágazatra.

Kivételt képez a tilalmak alól, ha a végfelhasználó számára konkrét választási lehetőséget kínáltak fel, és a GDPR értelmében a végfelhasználó megadta a hozzájárulását a konkrét adatkezeléshez.[24] (A hozzájárulás feltételeit a GDPR 7. cikke tartalmazza részletesebben.) Itt a DMA nagyon érdekes jogi megoldást használ A GDPR-ban szereplő hat jogalap, ha úgy tetszik, hat jogviszonytípus közül a legkevésbé értékeset, a legtörékenyebbet engedi csak meg a kapuőrnek.[25] Ha a végfelhasználó hozzá is járul az ilyen típusú adatkezelésekhez, akkor is bármi-

19 DMA 5. cikk (2) bekezdés a) pont.

20 DMA 5. cikk (2) bekezdés b) pont.

21 DMA (32) preambulumbekezdés.

22 DMA 5. cikk (2) bekezdés c) pont: „a releváns alapvető platformszolgáltatásokból származó személyes adatokat nem használhatja fel általa külön nyújtott egyéb szolgáltatások – például egyéb alapvető platformszolgáltatások – céljára, és fordítva."

23 DMA 5. cikk (2) bekezdés d) pont.

24 DMA 5. cikk (2) bekezdés d) pont.

25 A 6. cikk (1) bekezdése határozza meg a GDPR hat jogalapját, amelyek között első pontban említi a hozzájárulást.

kor visszavonhatja a hozzájárulását. Ettől értéktelen az ilyen jogviszony, üzleti modelleket ilyen bizonytalan jogalapra nem lehet építeni.

Milyen más lehetősége lenne a szolgáltatónak a GDPR alapján a DMA hiányában? Szerződésben írhatná elő az ilyen jellegű adatkezelések feltételeit megteremtő körülményeket, vagy akár a jogos érdekre is alapozhatná az adatkezelését. Bármelyiket is választaná (egyébként a vállalkozások ilyen helyzetben valószínűleg a szerződést választanák), a végfelhasználónak gyakorlatilag nem maradna alkupozíciója a magánszféráját érintő beavatkozás mértékét illetően. Tudatos döntés tehát a hozzájárulás egyedüli jogalapként való meghatározása a társjogalkotók részéről. Tehát a DMA itt is a GDPR eszközrendszerét veszi igénybe a piac szabályozásához.

1.4. Az üzleti felhasználókra vonatkozó szabályok

A kapuőrök által nyújtott platformszolgáltatásban megjelenő üzleti felhasználók rengeteg adatot szolgáltatnak a platformnak, mind saját maguk, mind a végfelhasználóik által. A DMA biztosítja, hogy ezekhez az adatokhoz az üzleti felhasználók is hozzáférjenek. Az üzleti felhasználók kérésére a kapuőrnek akadálytalan és ingyenes hozzáférést kell biztosítania ezekhez az adatokhoz. A kapuőröknek – akár alkalmazásprogramozó felülettel – elő kell segíteniük a valós időben történő hozzáférést az adatokhoz.[26] E hozzáférést a harmadik feleknek is meg kell adni abban az esetben, ha az üzleti felhasználó adatkezelőként jár el. A kapuőr nem használhat semmilyen szerződéses vagy egyéb korlátozást azért, hogy megakadályozza az üzleti felhasználókat a releváns adatokhoz való hozzáférésben, és lehetővé kell tennie a számukra, hogy az adatok lekérdezéséhez megszerezhessék a végfelhasználók hozzájárulását, ha ezt a GDPR és az elektronikus hírközlési adatvédelmi irányelv[27] előírja. A kapuőröknek lehetővé kell tenniük az üzleti felhasználók számára, hogy közvetlenül a végfelhasználóktól szerezzenek beleegyezést, vagy „más módon" kell megfelelniük az EU adatvédelmi szabályainak, beleértve az üzleti felhasználók anonimizált adatainak biztosítását.

1.5. A DMA adathordozhatósági rendelkezése

A DMA 6. cikk (9) bekezdése előírja, hogy a kapuőrök biztosítsák „a végfelhasználó által szolgáltatott vagy a végfelhasználó tevékenysége során keletkezett adatok hatékony hordozhatóságát a vonatkozó alap platformszolgáltatással összefüggésben". A DMA tehát adathordozhatósági kötelezettséget vezet be. Megköveteli a kapuőröktől, hogy a végfelhasználó és az üzleti felhasználó számára hozzáférést biztosítsanak a felhasználó által adott vagy a felhasználó tevékenysége során keletkezett adatokhoz, beleértve az ilyen adatokhoz való folyamatos és valós idejű hozzáférést.[28]

---

26 DMA (60) preambulumbekezdés.

27 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).

28 Julia Apostle: The EU's Digital Markets Act: What Does It Mean for Businesses and Data Privacy? *Orrick,* 2022. november 1., https://bit.ly/3RbJUUF.

Az érintettek ritkán gyakorolják a GDPR szerinti adathordozhatósághoz való jogukat, vagy pusztán információhiány miatt, vagy mert a GDPR csak természetes személyek személyes adataira vonatkozik, jogi személyekre (azaz tipikus „üzleti felhasználókra") nem. Kétségtelen, hogy a GDPR alkalmazásában az adathordozhatóság az egyik legkevésbé sikeres új jogintézmény. Természetes törekvésnek tekinthető, hogy a jogalkotó a GDPR szabályait konkretizálva, azokat kiegészítve pontosabb kötelezettségeket állapít meg egyes területeken, ahogyan azt teszi a DMA-ban is. Az adathordozhatóság joga az adatvédelmi jogban mindig is versenyjogi indíttatású rendelkezésként élt a szakmai köztudatban, amelynek révén a szolgáltatóváltás könnyebbé válik, és fontos eszköz lehet az online monopóliumok kialakulásának megelőzésében is.

Az idézett rendelkezés azt sugallja, hogy a DMA által rögzített kötelezettség kikövetkeztetett és származtatott adatokra is kiterjedhet. Tehát míg a GDPR kizárólag személyes adatokat szabályoz, addig a DMA által szabályozott adatok köre tágabb. Arra vonatkozóan, hogy az adat fogalma mennyiben tágabb a személyes adaténál, a DMA 2. cikk 24. pontja ad iránymutatást.[29] A kérdés az, hogy mit tud kezdeni az „egyszerű" felhasználó a szolgáltató által vele kapcsolatban kezelt, személyes adatnak nem minősülő metaadatokkal, úgy, hogy míg a GDPR a személyes adatok esetében előírja a szolgáltató által másik szolgáltató részére történő közvetlen továbbítás kötelezettségét,[30] addig a DMA szerinti adatok esetében ilyen előírást nem találunk. Felmerül a kérdés, hogy megfelel-e a nem csak személyes adatok hordozhatóságának biztosítása az arányosság elvének, azaz az idő- és a technológiai befektetéssel előállított adatok esetében is terheli-e a kapuőröket ez a kötelezettség. Végeredményben nem a kapuőrök innovációjának visszafogását fogja-e eredményezni ez a rendelkezés?[31] Ha ez bekövetkezne, az azt jelentené, hogy a szabályozás hatása (az adatkör tekintetében) túlontúl széles.

Egy másik elem miatt is jelentős a különbség a DMA és a GDPR között, ami hatással van az érintett adatok körére, ez pedig az adatok jogszerű kezelésének jogalapja, amelyen az adathordozhatósághoz való jog nyugszik.[32] A GDPR 20. cikk (1) bekezdése rögzíti, hogy az adathordozhatósághoz való jog csak azokra az adatokra terjed ki, amelyeket vagy szerződés, vagy hozzájárulás alapján kezelnek. Abban az esetben tehát nem kell az adathordozhatósághoz való jogot biztosítani, ha az adatkezelő jogos érdek alapján kezeli az adatokat. A DMA nem tartalmaz hasonló korlátozást, tehát a GDPR-hoz képest rugalmasabb szabályozást alkalmaz, és be is zár egy kiskaput arra az esetre, ha a platform másik jogalapra helyezné a szóban forgó adatkezelést.

Harmadrészt a DMA többletkötelezettséget állapít meg az adatkezelő kapuőrök számára, amikor a végfelhasználók felé történő adathordozhatósági intézkedéseket folyamatosan és valós idejű hozzáférés biztosításával írja elő. Ez szintén az adathordozhatóság GDPR szerinti szabályainak lényegi kiterjesztése, és olyan szolgáltatói fejlesztéseket kell indukáljon, amelyek túlmutatnak az adathordozhatóság intézményének európai előzményei által generált újításokon. An-

29 Az „aktusok, tények vagy információk bármilyen digitális megjelenítése, vagy az ilyen aktusok, tények és információk összeállításai, ideértve a hang-, kép- vagy audiovizuális felvétel formájában történő megjelenítést is."

30 GDPR 20. cikk (2) bekezdés.

31 Damien Geradin – Konstantina Bania – Theano Karanikioti: *The Interplay between the Digital Markets Act and the General Data Protection Regulation.* 2022, https://bit.ly/3SOPJc5.

32 Uo.

nál is inkább, mert – összhangban az adatmegosztási jogszabály (Data Act)[33] és a P2B rendelet[34] előírásaival, valamint az európai adatstratégia[35] célkitűzéseivel – a kapuőrök az üzleti felhasználók irányába is a felhasználókat illetőhöz hasonló adatszolgáltatási kötelezettséggel tartoznak, amihez számunkra nem tisztázott okból a jogalkotó a „folyamatos" és a „valós idejű" mellett hozzátette a „tényleges" és a „kiváló minőségű" jelzőket is.[36]

A DMA és a GDPR adathordozhatóságra vonatkozó rendelkezéseinek viszonyát a DMA (59) preambulumbekezdése hivatott rendezni, amely a félreértések elkerülése végett rögzíti: a kapuőr azon kötelezettsége, hogy biztosítsa az adatoknak a DMA szerinti tényleges hordozhatóságát, kiegészíti a GDPR szerinti adathordozhatósághoz való jogot. Erre tekintettel a legfontosabb kérdés az lehet, hogy a GDPR-ban meghatározott feltételeknek – ti. hozzájárulás vagy szerződéses jogalap, valamint automatizált adatkezelés – érvényesülniük kell-e a DMA szabályainak alkalmazásakor is. Az érintetti hozzájárulás szolgáltató általi beszerzése e tekintetben neuralgikus pontnak tűnik, hiszen a kapuőr által rögzített adatok (amelyek, visszautalva a korábban írtakra, tágabb halmaz képeznek az érintett személyes adatainak körénél) kezelése jelenleg egészen biztosan nem teljes egészében az érintett előzetes, önkéntes, konkrét, megfelelő tájékoztatáson alapuló hozzájárulásán alapul, és a szerződés teljesítéséhez való szükségességük is erősen megkérdőjelezhető. Mivel viszont ezen adatkör részét képezik a személyes adatnak nem minősülő adatok is, kérdés, hogy ezek kapcsán egyáltalán felmerülhet-e a GDPR szerinti érvényes jogalap meglétének szükségessége, és hogy milyen módon lesz lehetőség adott esetben a szolgáltató által a felhasználóról kezelt „adatcsomagot" szétválasztani személyes adatokra és személyes adatnak nem minősülő adatokra.

1.6. A DMA személyes adatokra vonatkozó egyéb rendelkezései

A kapuőrök kötelezettségei körében a DMA 6. cikk (11) bekezdése olyan kötelezettséget ír elő a kapuőrök számára, amely szerint „az online keresőprogramokat nyújtó, harmadik félnek minősülő vállalkozások kérésére tisztességes, észszerű és megkülönböztetéstől mentes módon hozzáférést kell biztosítania számukra a kapuőr online keresőprogramjával végzett díjmentes és fizetett keresések során a végfelhasználók által generált rangsorolási, keresési, kattintási és megtekintési adatokhoz".

Fontos, hogy a DMA szövege értelmében az ilyen adatszolgáltatás keretében a személyes adatnak minősülő keresési, kattintási és megtekintési adatokat anonimizálni kell.[37] A DMA az „anonimizálás" (anonymised) szót használja, és bár nem definiálja a fogalmat, vélhetően ez a

33 Javaslat. Az Európai Parlament és a Tanács rendelete a méltányos adathozzáférésre és adatfelhasználásra vonatkozó harmonizált szabályokról (adatmegosztási jogszabály) (Data Act).

34 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 (P2B rendelet).

35 Az Európai Bizottság összefoglalója az európai adatstratégiáról: https://bit.ly/46rPZ3G.

36 A DMA és a GDPR adathordozhatósági előírásaiban közös elem, hogy azokat a szolgáltatóknak díjmentesen kell végrehajtaniuk.

37 DMA 6. cikk (11) bekezdés.

GDPR „anonim információk" fordulatának feleltethető meg.[38] Ahogyan fentebb említettük, a DMA tartalmazza a nem személyes adat fogalmát is – ez felel meg az adatvédelmi jogban ismert anonimizált adat fogalmának. Olyan adatokról van szó, amelyek nem köthetők meghatározott természetes személyhez, ennélfogva nem terjed ki rájuk a személyes adatok védelme. Az adatok anonimizálása nem feltétlenül magától értetődő, rutinszerűen végrehajtott műveletet jelent, hiszen számolni kell a nagy és összetett adatbázisok „deanonimizálásának" kockázatával. Az anonimizálás tehát mindig a technológia adott lehetőségeinek fényében értékelendő, és jelentős piaci értéket vonhat el, ha a visszaállíthatóság elkerülése érdekében a megfelelő intézkedéseket elvégzik.[39]

A DMA által szabályozott adatokat illetően a rendelet a kapuőrökre vonatkozó szabályok elavulása ellen ható rendelkezésként a rájuk vonatkozó kötelezettségek aktualizálására is gondol, amikor a 12. cikkben kitér arra, hogy a Bizottság megkapja a felhatalmazást, hogy jogi aktusokat fogadjon el az 5. és 6. cikkben megállapított kötelezettségek tekintetében. Így a 12. cikk (2) bekezdés e) pontja rögzíti, hogy az új jogi aktus hatálya kibővíthető a bizonyos típusú adatokra vonatkozó valamely kötelezettségnek más típusú adatokra való kiterjesztésével. Ez pedig a jövőben érintheti a GDPR által is szabályozott személyes adatokat is.

A fentiekben elemzett szabályok kikényszerítését a jogalkotó egy kézben összpontosítja: az Európai Bizottsághoz telepíti a legtöbb hatáskört, és minimális teret hagy a tagállami hatóságok számára. Lehetséges, hogy a jogalkotó a GDPR egyik tanulságát vette itt alapul, ugyanis annak kikényszerítése rendkívüli erőfeszítéseket követel egyes tagállami hatóságoktól, míg mások – a gazdasági koncentráció egyenetlensége okán – jóval kevesebb eljárásban vesznek részt fő felügyeleti hatóságként. Feltehetően ennek a feltorlódásnak az elkerülése volt az egyik érv a jogalkotó oldalán az új kikényszerítési modell mellett.[40]

2. Versenyképes digitális gazdaság versus a magánszféra védelme

Legkésőbb a 2010-es végek végére egyértelművé vált, hogy a technológiai fejlődés és az annak minden előnyét kiaknázni kívánó gazdasági szereplők által nyújtott szolgáltatások egy sor olyan kihívással szembesítik a világ jogalkotó szerveit, amelyek azonnali reakciót és egyes korábban követett alapvető szabályozási elvek átgondolását igénylik. E folyamatokon még jobban gyorsított a globális pandémiás helyzet, amikor még több, korábban személyes interakciót kívánó tevékenység és üzleti aktus költözött az online térbe.

Míg korábban az európai uniós szabályozás sarokkövének számított a személyes adatok és a magánszféra alapjogi szintű védelme, addig mára szintén prioritássá vált az EU számára az

38 A nem személyes adatok Európai Unióban való szabad áramlásának keretéről külön rendelet szól (2018/1807), de erre a rendeletre sem utal a DMA.

39 Az ilyen adatbázisok az MI számára kínált tanulási adatok értékét jelentősen csökkentik. Philipp Hacker – Johann Cordes – Janina Rochon: *Regulating Gatekeeper AI and Data: Transparency, Access and Fairness under the DMA, the GDPR and Beyond,* https://bit.ly/3MVNOyy, 30.

40 Suzanne Vergnolle: *Enforcement of the DSA and the DMA: What did We Learn from the GDPR?* Hal Open Science, https://bit.ly/49H6bky, 103.

adatalapú gazdaság nóvumainak kiaknázása, az európai piacok versenyképességének növelése, ahogy erre az európai adatstratégia egyértelműen utal. Ez az ellentmondás tetten érhető az uniós jogalkotás legfrissebb európai adatstratégia termékein és a kodifikáció irányain. Így például a Data Act célja az európai adatgazdaság dinamizálása, míg az „ikerrendeletek", a DMA és a DSA célja a szolgáltatók keretek közé szorítása, ezzel párhuzamosan pedig a GDPR szerinti érintetti jogok érvényesítéséhez szükséges garanciák biztosítása. Egyértelmű elmozdulás érzékelhető a korábban a magánszféra védelmét mindenek felettinek tekintő EU-s jogalkotástól. A felhasználói adatok gazdasági értékét immár senki sem vonja kétségbe, még ha például a Facebook „ingyenességét" vitató hatósági álláspontok nem is egyeznek minden esetben a tagállami bíróságokéival.[41] Onnantól fogva pedig, hogy az elérhetőségi adatokra és a felhasználói preferenciákra nem mint titkokra, hanem gazdasági értékkel bíró erőforrásokra tekintünk, számtalan kérdés és lehetséges szabályozási irány merül fel.

Eddig ezen adatok szisztematikus feldolgozásából és hasznosításából elsődlegesen a szolgáltató profitált, de az elmúlt időszakban jogosan merült fel az igény, hogy azok váljanak hozzáférhetővé a felhasználók számára is. Ennek oka lehet a már említett magánszféra-védelem, ti. hogy az érintett pontosan ismerje, milyen adatokat kezel vele kapcsolatban a szolgáltató. De ugyanígy legitim igény lehet az összegyűjtött adatok „átvitele" más szolgáltatóhoz, akár a felhasználó adminisztrációs terheit könnyítendő (adathordozhatóság), akár más – például gazdasági – célból. A platformszolgáltatások esetében az üzleti felhasználók is joggal tették szóvá, amikor az általuk kínált szolgáltatások útján megszerzett adatokat a platformszolgáltató a saját üzleti céljaira használta, sokszor olyan technológiát alkalmazva, amely éppen az adatkezelőként felelősséget vállaló üzleti felhasználókat zárta ki az adatok megismeréséből.

A GDPR 2018-as hatálybalépése után elsődlegesen az érintetti jogok és az adatkezelői kötelezettségek által kínált eszköztár szolgált az adatkezelők mozgásterének kijelölésére, azonban az elmúlt időszak európai uniós jogalkotási termékei arra utalnak, hogy az EU azonosított néhány neuralgikus pontot, amely sürgős és pontos beavatkozást igényel. Az adathordozhatóság a GDPR-ban még inkább csak elméleti síkon létező jogintézmény volt, de immáron egyértelműen azonosítható cél, hogy nagyobb hangsúlyt kapjon az érintetti jogok között. Szintén világos szabályozói kívánalom a „vevő fogva tartás" egyes eseteinek megakadályozása e jogintézmény erősítésével. Ezzel párhuzamosan az ágazatok közötti horizontális adatmegosztás, így különösen az internet of things (IoT) által generált adatok hasznosítása és a bennük rejlő lehetőségek maximális kihasználása is megjelenik a Data Act rendelkezései formájában.

A fentiek alapján egyértelmű, hogy az egyes EU-s jogalkotási termékek a digitális gazdaság eltérő szegmenseit érintik, és sokszor egymással látszólag nem minden esetben kompatibilis célok elérését kívánják, mégis egyfajta szabályozási univerzummá állnak össze. A kérdés az, hogyan oldható meg a jogalkotói céloknál, hogy a kecske is jóllakjon és a káposzta is megmaradjon, és egyáltalán tudnak-e ezek a szabályozások úgy együtt létezni, hogy bizonyos esetekben nem oltják ki egymást.

41 Lásd Fővárosi Törvényszék 105.K.701.043/2020/14.; Kúria Kfv.37.243/2021/11.

3. A szabályozási univerzum

Ahhoz, hogy az előzőekben felvázolt szabályozási rendszer elemei közötti összefüggéseket, így különösen a DMA és a GDPR szabályai közötti viszonyrendszert értelmezni tudjuk, elengedhetetlen röviden áttekinteni – természetesen a jogszabályok tartalmának tételes ismertetése nélkül – azok legfőbb tartalmi elemeit és a megalkotásuk mögött húzódó, deklarált jogalkotói célokat.

3.1. A Data Act

A bemutatott jogalkotási termékek közül a jelenleg a brüsszeli jogalkotási mechanizmus malmai között őrlődő Data Act is lépést kíván tenni az adatalapú európai gazdaság dinamizálása irányába. Ezt támasztja alá a Bizottság kapcsolódó sajtóközleménye,[42] a digitális átalakulás utolsó horizontális építőköveként hivatkozva a rendelettervezetre, amely kulcsszerepet fog játszani a 2030-ra elérendő digitális célok megvalósításában. A rendelettervezet preambulumának szövegét olvasva az a benyomásunk támadhat, hogy az EU, hallgatva az új idők szavára, a mára kissé megmerevedett korábbi jogi struktúrán kíván áramvonalasítani és igazodni a technológia jelenlegi állásához. Így például a tervezet rögzíti, hogy ösztönzi az algoritmusok használatát és az adatvédelmi előírások tiszteletben tartását az adatmegosztások során. Az európai adatvagyonnal kapcsolatos gondolkodásmód változására utal az is, hogy a tervezet egyes rendelkezései a személyes adatok kategóriáján túlmutató, a nem személyes adatokat is magában foglaló szabályozási tárgyra vonatkozóan kerülnek megfogalmazásra. A tervezet talán legfontosabb eleme az adatok kezelésében részt vevő „adattulajdonos", „adatkezelő", „felhasználó" és „gyártó" kifejezés bevezetése és változatos használata, egyúttal e relációban az egyes felek jogainak és különösen kötelezettségeinek a differenciálása. Jelenlegi formájában azonban épp e minőségek pontos definiálásával marad adós a tervezet szövege.

A rendelettervezet 1. cikke rögzíti, hogy a rendelet nem érinti a személyes adatok védelmére vonatkozó uniós jog – különösen a GDPR és az elektronikus hírközlési adatvédelmi irányelv – alkalmazhatóságát, így a felügyeleti hatóságok hatáskörét és illetékességét sem. A tervezet a vállalkozások és a fogyasztók, valamint a vállalkozások közötti adatmegosztás szabályait részletező II. fejezetének előírásai körében rögzíti, hogy az e fejezetben meghatározott jogok tekintetében – ha a felhasználó az e fejezet szerinti jogok és kötelezettségek hatálya alá tartozó személyes adatok érintettje – a rendelet kiegészíti a GDPR 20. cikke szerinti adathordozhatósághoz való jogot. Annál is inkább igaz ez, mivel a Data Act valóban az adathordozhatóságnak a GDPR-ban megalkotott jogintézményét igyekszik gyakorlati oldalról megközelítve, részletszabályok tisztázásával pontosítani.

Ennek kapcsán a GDPR 20. cikk (1) bekezdése akképp rendelkezik, hogy az érintett jogosult tagolt, széles körben használt, géppel olvasható formátumban megkapni az adatkezelő által vele kapcsolatosan kezelt személyes adatokat, ha az adatkezelés jogalapja az érintett hozzájárulása vagy olyan szerződés teljesítése vagy előkészítése, amelynek egyik szerződő fele az érintett.

---

42 Európai Bizottság: *Data Act: Commission proposes measures for a fair and innovative data economy* (sajtóközlemény), https://bit.ly/3uttGNV.

További feltétel, hogy az adatkezelés automatizált módon történjen. Ehhez képest a Data Act szerint az adattulajdonosnak – vagyis az adatok hozzáférhetővé tételét célzó jogi kötelezettségek alanyának – indokolatlan késedelem nélkül, ingyenesen, az adattulajdonos rendelkezésére állóval megegyező minőségben és adott esetben folyamatosan és valós időben kell az érintett vagy harmadik fél rendelkezésére bocsátania a termék vagy a kapcsolódó szolgáltatás használata révén generált adatokat.[43]

A Data Act tervezete a fentieken túl – igazolva az uniós szabályozási „univerzumra" tett utalásunkat – hivatkozza a DMA által bevezetett kapuőr minőséget, amikor e szolgáltatókra többletkötelezettséget telepít, ti. semmilyen módon – többek között pénzbeli vagy egyéb ellentételezés nyújtásával – nem hívhatják fel vagy ösztönözhetik üzletileg a felhasználókat arra, hogy a Data Act által meghatározott adathordozhatóságra vonatkozó jogaikat gyakorolva személyes adataikat a kapuőr valamely szolgáltatása rendelkezésre bocsássák vagy más szolgáltatót a személyes adatok kapuőrnek való átadására kérjék. A tervezet még tovább megy, és azt is megtiltja, hogy a kapuőr bármilyen módon olyan adatokhoz jusson a felhasználótól, amelyekre a felhasználó az adathordozhatóságnak a Data Act szerinti gyakorlása útján tett szert. Ez utóbbi rendelkezés esetében felmerülhetnek bennünk kételyek a szabályozás gyakorlati kivitelezhetőségével és betarthatóságával kapcsolatban. A jogszabálytervezettel kapcsolatos általánosabb kritikák arra mutatnak rá, hogy az abban foglaltak betartatásával az EU túl drasztikusan nyúlna bele az adatpiac természetesen alakuló versenydinamikájába, egyúttal csökkentené e szolgáltatásoknak a felhasználói igényekhez való igazodási képességét.[44]

Az adathordozhatóság jogának zászlóra tűzése deklaráltan nem csak az adatkezelések érintettjei irányába tett jogalkotói gesztus. Ahogy a rendelettervezet preambulumában is megjelenik, az EU észlelte, hogy a jelenlegi digitális piaci ökoszisztémában az induló vállalkozások, a kis- és középvállalkozások, valamint a hagyományos ágazatokban működő, kevésbé fejlett digitális képességekkel rendelkező vállalkozások nehezen férnek hozzá a releváns adatokhoz, mivel azok kis számú, az adatok monetizálásához szükséges technológiai infrastruktúra révén számottevő gazdasági erővel bíró vállalat kezében összpontosulnak. A Data Act deklarált célja, hogy megkönnyítse az ilyen entitások hozzáférését a DMA-ban kapuőrként definiált techóriások által kezelt adatokhoz, egyúttal biztosítsa, hogy a kapcsolódó kötelezettségek hatókörét a hatáskörtúllépés elkerülése érdekében a lehető legarányosabban alkalmazzák.

3.2. A P2B rendelet

A technológiai és információs erőfölénnyel rendelkező vállalatok előnyének kiegyenlítése és a mikro-, kis- vagy középvállalkozások érdekei érvényesítésének elősegítése mint jogalkotói cél megjelenik egy másik jelentős uniós jogalkotási vívmányban, a P2B rendeletben is. A Bizottság

---

43 A rendelkezésre bocsátás módját nem határozza meg konkrétan a szöveg, így nem feltétlenül jelenti ez az adatok tényleges átadását. Lásd Moritz Hennemann et al.: *The Data Act Proposal: Literature Review and Critical Analysis, Part I.* Passau, University of Passau, 2023, 31.

44 Sean F. Ennis – Ben Evans: Cloud Portability and Interoperability under the EU Data Act: Dynamism Versus Equivalence. *SSRN,* 2023. március 22., https://bit.ly/3t51yAf, 18.

a rendelet javaslatához fűzött indokolásában hangsúlyozta a vállalkozások bizonyos online szolgáltatásoktól való függőségét, ami magában foglalja, hogy az online közvetítő szolgáltatók számos olyan potenciálisan káros kereskedelmi gyakorlatba bonyolódhatnak, amely korlátozza az üzleti felhasználók rajtuk keresztül történő értékesítéseit, és azt kockáztatják, hogy megrendül a beléjük vetett bizalom. E káros gyakorlatok témánkat érintő megnyilvánulási formája a P2B rendelet előírásai által is nevesített olyan szolgáltatói magatartás, amelynek során az üzleti felhasználók nem férnek hozzá a saját ügyfeleik azon adataihoz, amelyeket az általuk nyújtott szolgáltatással kapcsolatban gyűjtött be az online közvetítő szolgáltató, vagy nem átlátható számukra, mit is kezd pontosan a közvetítő szolgáltató ezekkel az adatokkal.

Ezért az online közvetítő szolgáltatóknak szerződéses feltételeikben tájékoztatást kell nyújtaniuk üzleti felhasználóik számára arról a hozzáférésről, amellyel a szolgáltató vagy a szolgáltató irányítása alatt álló üzleti felhasználó vagy kereskedelmiweboldal-használó rendelkezhet bármely olyan személyes adatra, más adatra vagy mindkettőre vonatkozóan, amelyeket az üzleti felhasználók, a kereskedelmiweboldal-használók vagy a fogyasztók bocsátanak rendelkezésre az érintett online közvetítő szolgáltatás vagy online keresőprogram igénybevételéért vagy amelyek e szolgáltatások nyújtása során keletkeznek. A P2B rendelet tehát egyértelműen korlátok közé szorítja a közvetítő szolgáltatókat, amikor tételes tájékoztatási kötelezettséget ír elő nekik arról, hogy az üzleti felhasználóiknak nyújtott szolgáltatások kapcsán milyen személyes adatok birtokába jutnak és mit tesznek azokkal. Elvárás, hogy az üzleti felhasználó tisztában legyen például azzal, hogy a közvetítő szolgáltató hozzáfér-e az üzleti felhasználóval szerződő fogyasztók személyes adataihoz, és ha igen, az adatok mely kategóriáihoz, valamint azokat átadja-e harmadik felek részére.

A platform-to-business rendelet tehát különböző olyan intézkedések elvégzésének kötelezettségét rója a közvetítő szolgáltatókra, amelyek célja, hogy az üzleti felhasználóik számára átláthatóbb legyen az adatkezelésük, azért, hogy ezek az intézkedések hozzájáruljanak az adatok nagyobb mértékű megosztásához, valamint fokozzák azokat az erőfeszítéseket, amelyek az innováció és a növekedés kulcsfontosságú forrását jelentő közös európai adattér megvalósítására irányulnak.[45] Azt látjuk tehát, hogy míg korábban az európai jogalkotás hangsúlya az érintettek (felhasználók) tájékoztatásán és az irányukba tanúsított szolgáltatói transzperencián volt, addig immáron a nagy techcégek a velük szemben kiszolgáltatott helyzetben lévő üzleti felhasználóik irányába is tételes elszámolási kötelezettséggel tartoznak arról, hogy milyen műveleteket végeznek az üzleti felhasználók ügyfeleinek a birtokukba kerülő személyes adataival.

3.3. A Bundeskartellamt kontra Facebook-ügy

Versenyjogi szempontból rövid értékelést igényel az a német versenyhatósági döntés,[46] amely a Facebook szolgáltatói adatkumulációra visszavezethető visszaélései tárgyában született, és az uniós jogalkotóknak vélhetően ihletadó forrásként, de legalábbis szándékaik helyességének iga-

45 P2B rendelet (35) preambulumbekezdés.

46 Case Summary: Facebook, Exploitative business terms pursuant to Section 19(1) GWB for inadequate data processing, B6-22/16. *Bundeskartellamt,* 2019. február 15., https://bit.ly/40QUvYp.

zolására szolgált a DMA tervezetének szövegezése során.[47] 2019. februári döntésében a Bundeskartellamt (német szövetségi versenyhatóság) jogellenesnek, erőfölénnyel visszaélő és kizsákmányoló jellegűnek ítélte a Facebooknak azt a gyakorlatát, amely szerint a felhasználók csak azzal a feltétellel használhatták a közösségi oldalt, hogy a Facebook a saját weboldalán kívül is gyűjthet felhasználói adatokat az interneten vagy okostelefonos alkalmazásokban, és ezeket az adatokat a felhasználó Facebook-fiókjához rendelheti.

A döntésben a hatóság kötelezte a Facebookot, hogy a jövőben az általa közvetlenül nyújtott szolgáltatáson kívül gyűjtött összes adat kezeléséhez szerezze be előzetesen az érintett felhasználók hozzájárulását. A szolgáltató a döntés ellen fellebbezett, aminek a düsseldorfi tartományi felsőbíróság közbenső ítéletében helyt is adott, lényegében arra alapítva érvelését, hogy a felhasználók megismerhetik a Facebook használatával járó előnyöket és hátrányokat, valamint befolyásmentesen dönthetnek arról, hogy e feltételek alapján a szolgáltató rendelkezésére bocsátják-e személyes adataik széles halmazát. Az ügy újabb fordulatot a német szövetségi legfelső bíróságon vett, amely KVR 69/19 számú, 2020. június 23-i határozatában hatályon kívül helyezte a düsseldorfi bíróság határozatát, és elutasította a panasz halasztó hatálya iránti kérelmet. Ezt követően a düsseldorfi bíróság 2021 márciusában előzetes döntéshozatal iránti kérelmet nyújtott be az Európai Unió Bíróságához (EUB).[48]

Nem túlzás történelmi jelentőségűnek minősíteni az ügyet, ha az EUB ki fogja jelölni döntésében a versenyjog és az adatvédelmi jog intézményrendszere közötti határokat,[49] vagy éppenséggel amellett érvel, hogy azok együttes alkalmazása, így a piaci magatartások értékelése során szükséges figyelembe venni az adatvédelmi szempontokat[50] Az EUB honlapján elérhető legutóbbi indítvány a versenyhatóság érvelésének nagy részét magáévá tevő álláspontot sejtet.[51]

A német versenyhatósági döntés érvelése előbb a német, majd az európai igazságszolgáltatás malmai között csiszolódott – és vett fel egy ponton egészen meglepő formát –, viszont az időközben hatályba lépő DMA-val annyiban okafogyottá vált az eljárás, hogy a rendelet 5. cikk (2) bekezdése egyértelműen tilalmazza a kapuőrök számára, hogy az általuk nyújtott szolgáltatásokból származó személyes adatokat összekapcsolják más, általuk nyújtott szolgáltatásokból származó vagy harmadik fél szolgáltatásából beszerzett személyes adatokkal. Emellett ezeket az adatokat nem használhatják fel általuk külön nyújtott egyéb szolgáltatások – például egyéb alapvető platformszolgáltatások – céljára és fordítva, továbbá a végfelhasználókat nem is léptethetik be más szolgáltatásaikba személyes adatok összekapcsolása céljából.

---

47 A különböző szolgáltatások nyújtása útján beszerzett személyes adatok adatbázisai összekapcsolásának számtalan előzménye van az európai versenyjogban. E kérdéskör állatorvosi lova volt a Facebook–WhatsApp-fúzió 2014-ben és az Európai Bizottság ezzel kapcsolatos döntései: https://bit.ly/49SwLrd.

48 A C-252/21. Meta Platforms és társai (Conditions générales d'utilisation d'un réseau social) ügyben az előzetes döntéshozatali kérelemmel kapcsolatos dokumentum.

49 Wouter P. J. Wils: *The Obligation for the Competition Authorities of the EU Member States to Apply EU Antitrust Law and the Facebook Decision of the Bundeskartellamt.* London, King's College London Law School, 2019, 14–15.

50 Anne C. Witt: The Digital Markets Act: Regulating the Wild West. (60)3 *Common Market Law Review* (2023) 625–666.

51 C-252/21. Meta Platforms és társai (Conditions générales d'utilisation d'un réseau social), https://bit.ly/47Mclhz.

4. Az adatmegosztások a DMA alatt és a GDPR szerinti hozzájárulás szerepe

Az adatmegosztás a DMA-ban az online hirdetési piacok, pontosabban a célzott hirdetések miatt került fókuszba, mégpedig az imént ismertetett német Facebook-ügy miatt.[52] Ez volt az első eset, amikor az adatvédelmi jog megsértése kizsákmányoló típusú erőfölénnyel való visszaélést eredményezett. Emögött az a német bírósági gyakorlat húzódik meg,[53] amely szerint tisztességtelen olyan szerződéses kikötés egyoldalú alkalmazása, amely más hatályos jogszabályokkal összeegyeztethetetlen és erőfölénnyel való visszaélést valósít meg, ha ez a képesség kifejezetten az érintett vállalkozás domináns pozíciójából fakad.

Ez a megközelítés már megjelent a német és a francia versenyhatóság közös 2016-os tanulmányában, amelyben úgy foglaltak állást, hogy ha az erőfölényes vállalkozás adatvédelmi jogsértést követ el, és a kettő között (az erőfölényes pozíció és az adatvédelmi jogsértés között) szoros összefüggés van, akkor az erőfölénnyel való visszaélést alapoz meg.[54] A német hatóság nem az uniós, hanem a német versenyjogot alkalmazta. Az 1/2003/EK rendelet[55] 3. cikk (2) bekezdése egyébként megengedi a szigorúbb nemzeti jogalkalmazást az erőfölénnyel való visszaélés kapcsán. Igaz, az európai versenyjogi gyakorlattól sem idegen, hogy erőfölénnyel való visszaélést állapítson meg, amikor a domináns szereplő visszaél valamilyen szabályozással és azzal versenyellenes hatást idéz elő.[56] Végül azonban a fenti német jogalkalmazási megközelítés az európai uniós versenyjog elismerését jelenti, azzal, hogy ilyen jelentős elem, mint a kapuőri adatösszekapcsolás tilalma bekerült a DMA 5. cikk (2) bekezdésébe és a 6. cikk (2) bekezdésébe is.

Ezek a rendelkezések a kapuőröknek az adatokhoz való hozzáférését szorítják keretek közé. Bár a DMA kifejezetten rögzíti, hogy nem érinti a GDPR-t,[57] a német Facebook-ügy alapján az 5. cikk (2) bekezdése mégis szűkíti a kapuőrök esetében a GDPR adatkezelési jogalapra való hivatkozásának körét, amikor az adatösszekapcsolást és kereszthasználatot kifejezetten a GDPR 6. cikk (1) bekezdése szerinti jogosulti hozzájárulásra szűkíti, és kizárja a kapuőr esetében a szerződés teljesítésére [b) pont] és a jogos érdekre [f) pont] való hivatkozást.[58] A DMA szerint[59] amikor a kapuőr hozzájárulást kér, akkor a GDPR szellemében proaktívan nyújtania kell a végfelhasználó számára egy felhasználóbarát megoldást, amellyel az kifejezett, világos és egyértelmű módon megadhatja, módosíthatja vagy visszavonhatja hozzájárulását. A DMA 5. cikk (2) bekezdése alapján, ha az első alpont alkalmazásában adott hozzájárulást a

---

52 Geradin–Bania–Karanikioti i. m. (31. lj.); *Bundeskartellamt Prohibits Facebook from Combining User Data from Different Sources,* 2019, https://bit.ly/46u3LTI.

53 VBL-Gegenwert II., Hintergrundinformationen zum Facebook-Verfahren des Bundeskartellamtes, 2017, https://bit.ly/49ILNQh.

54 Autorité de la Concurrence – Bundeskartellamt: *Competition Law and Data,* 2016. május 10., https://bit.ly/40T3c4r, 25.

55 A Tanács 1/2003/EK rendelete (2002. december 16.) a Szerződés 81. és 82. cikkében meghatározott versenyszabályok végrehajtásáról.

56 C-457/10. AstraZeneca kontra Commisson.

57 DMA (37) preambulumbekezdés.

58 DMA (36) preambulumbekezdés.

59 DMA (37) preambulumbekezdés.

végfelhasználó megtagadta vagy visszavonta, a kapuőr ugyanarra a célra egy éven belül nem ismételheti meg egynél többször a hozzájárulás iránti kérelmét. Az érintetteket a hozzájárulásuk megadása előtt tájékoztatni kell az adatkezelés és -felhasználás tervezett céljairól, és lehetőséget kell nekik biztosítani arra, hogy minden egyes célhoz a hozzájárulásukat adhassák vagy megtagadhassák azt.[60]

A DMA szerint a kapuőröknek lehetővé kell tenniük, hogy a végfelhasználók szabadon dönthessenek az adatkezelési és a beléptetési gyakorlatok elfogadásáról, mégpedig olyan módon, hogy kisebb mértékű személyre szabással járó, de egyenértékű alternatívát kell kínálniuk anélkül, hogy az alapvető platformszolgáltatásnak vagy egyes funkcióinak az igénybevételét a végfelhasználó hozzájárulásától tennék függővé.[61] A kisebb mértékű személyre szabással járó alternatíva nem lehet eltérő vagy rosszabb minőségű a hozzájáruló végfelhasználóknak nyújtott szolgáltatáshoz képest, kivéve, ha a minőség romlása közvetlenül abból adódik, hogy a kapuőr nem kezelheti az ilyen személyes adatokat vagy nem tudja beléptetni a végfelhasználókat egy szolgáltatásba. A végfelhasználónak tájékoztatást kell kapnia arról, hogy a hozzájárulás megtagadása kisebb mértékben személyre szabott ajánlathoz vezethet, egyebekben azonban az alapvető platformszolgáltatás változatlan marad. A hozzájárulás megtagadása ugyanakkor nem lehet nehezebb, mint a hozzájárulás megadása.[62]

Nem zárja ki azonban a DMA 5. cikk (2) bekezdése, hogy a kapuőr a GDPR 6. cikk (1) bekezdés c), d) vagy e) pontjára (jogi kötelezettség teljesítésére, létfontosságú érdekek védelmére, továbbá közérdekű vagy az adatkezelőre ruházott közhatalmi jogosítvány végrehajtásához szükséges intézkedésre) hivatkozzon. Ez, értelmezésünk szerint, a kapuőr által kezelt adatokhoz való hozzáférés szempontjából bír jelentőséggel, például amikor a kapuőr a felhasználók adatainak védelmére hivatkozással akarja versenytársai hozzáférését korlátozni, mint a Google Sandbox ügyben, amelynek tárgya az volt, hogy a Google kizárta a harmadik fél nyomkövető sütijeit a Chrome böngészőből.[63] Ez a döntés tehát továbbra sem akadályozhatja, hogy az online hirdetési piacon a versenytársak hozzáférjenek a Google által kezelt adatokhoz, mert különben a Google erőfölénnyel való visszaélést követne el, így a GDPR 6. cikk (1) bekezdés c) pontja szerinti adatkezelési jogalap alkalmazható lehet, amennyiben ezek az adatok személyes adatnak minősülnek.

A GDPR 20. cikk (1) bekezdése rögzíti, hogy az adathordozhatósághoz való jog csak azokra az adatokra terjed ki, amelyeket szerződés vagy hozzájárulás alapján kezeltek. Ez a korlátozás azonban a DMA 6. cikk (9) bekezdése alapján nem vonatkozik a kapuőrök által kezelt végfelhasználói adatokra, amelyek hordozhatóságát a kapuőröknek attól függetlenül biztosítaniuk kell, hogy azok kezelése hozzájáruláson vagy szerződésen kívüli jogalap alapján történik.[64]

---

60 European Data Protection Board, Guidelines 05/2020 on consent under Regulation 2016/679, Version 1.1., 2020. május 4., 55–61. bekezdés.

61 DMA (36) preambulumbekezdés.

62 DMA (37) preambulumbekezdés.

63 Lásd Investigation into Google's 'Privacy Sandbox' browser changes. *Competition and Markets Authority,* 2021. január 8., https://bit.ly/3RcifTP.

64 Konstantina Bania: Fitting the Digital Markets Act in the Existing Legal Framework: The Myth of the „Without Prejudice" Clause. 19(1) *European Competition Journal* (2022) 116–149., https://doi.org/10.1080/17441056.2022.2156730, 18.

Más a helyzet azonban, amikor az adathordozást nem a felhasználó, hanem olyan üzleti felhasználó kezdeményezi, amelynek a szolgáltatását a felhasználó a kapuőr platformján keresztül veszi igénybe. Ebben az esetben a DMA 6. cikk (10) bekezdése alapján a személyes adatokhoz való hozzáférés csak akkor adható meg, ha a végfelhasználó a „hozzájárulásával belegyezik az ilyen megosztásba".

5. A DMA és az európai adatvagyon megőrzése

Ha a digitális gazdaság legfontosabb alapanyaga az adat,[65] akkor megállapítható, hogy az európai adatok 92 százalékát az Egyesült Államokban kezelik, és azokhoz az amerikai kormányzati szerveknek hozzáférésük lehet.[66] Ha az adat az új olaj,[67] akkor természetesen az, aki birtokolja őket, jelentős hatalmat tudhat a magáénak.[68] Kína az adatvagyonát lényegében nemzeti stratégiai értéknek tekinti, ezért teljes állami felügyeletet gyakorol felettük az egyéni jogok védelmének figyelmen kívül hagyásával, míg az Egyesült Államokban ezen a téren is a magánszféráé a döntő szerep a jelentős piaci koncentráltság mellett.[69] Az amerikai technológiai óriások zéróáras (az ingyenesség látszatára építő) üzleti modellje az Egyesült Államokba szívja az európai adatvagyont, ami nem csak további üzletszerzésre használható fel. Az EUB 2020 júliusában hozott ítélete meg is erősíti ezt az aggodalmat.[70]

Ebben az ítéletében az EUB megállapította, hogy az EU és az Egyesült Államok közötti adatvédelmi pajzs keretrendszere már nem megfelelő mechanizmus az EU adatvédelmi követelményeinek való megfeleléshez a személyes adatoknak az Európai Unióból az Egyesült Államokba való továbbítása vonatkozásában. Az EUB szerint ugyanis nem biztosított a GDPR és az EU Alapjogi Charta által a személyes adatokat illetően rögzített védelmi szint, mert az uniós adatok jogosultjainak nem áll rendelkezésükre hatékony védelmi mechanizmus, ha az amerikai felhasználás sérti az EU jogában létező és elismert jogaikat, például az adataik amerikai kormányzati felhasználása esetén. Az európai adatvagyonnak az Egyesült Államokba vándorlása többek között a mesterséges intelligencia (MI) kifejlesztése és felhasználása terén folytatott nagy nem-

65 Opinion 8/2016 EDPS Opinon on coherent enforcement of fundamental right sin the age of big data, 2016. szeptember 23., 6.

66 Samuel Stolton: LEAK: Commission in Bid for EU Data Sovereignty with Digital Decade Targets. *Euractive,* 2021. március 8., https://bit.ly/46InNtT; Sean Fleming: What is Digital Sovereignty and Why is Europe So Interested in it? *World Economic Forum,* 2021. március 15., https://bit.ly/47ogGI3.

67 The World's Most Valuable Resource Is No Longer Oil, but Data. *The Economist,* 2017. május 6., https://econ.st/47rUw7R.

68 François Candelon – Martin Reeves: The New Digital World: Hegemony or Harmony? *BCG,* 2017. november 14., https://on.bcg.com/47lK7dI.

69 A European strategy for data. Communication from the Commission to European Parliament, European Council, the Council, the European Economic and Social Committee, the Committee of the Regions, Brussels, 19.2.2020 COM(2020) 66 final, 3.

70 Lásd bővebben C-311/18 Facebook Ireland és Schrems [183]–[184].

zetközi versenyfutásban is károsnak bizonyult.[71] Az adatok ugyanis mennyiségi és minőségi szempontból is meghatározók az MI működése szempontjából.[72]

Az európai adatok tehát jelenleg a zéróáras üzleti modellnek köszönhetően az amerikai technológiai cégeket erősítik. Ebből a szempontból kérdés, milyen hatással van a DMA az európai adatvagyon megőrzésére. Ez a hatás elsősorban a reklámok célzásához szükséges adatokhoz való hozzáférés szabályozása szempontjából vizsgálható. Megállapítható, hogy a DMA emeli a reklám célzásához szükséges adatgyűjtés költségét azzal, hogy az 5. cikk (2) bekezdése kizárólag a kifejezett hozzájárulást ismeri el mint jogalapot a GDPR 6. cikk (1) bekezdésében felsorolt jogalapok közül, hogy a kapuőrök a felhasználók különböző forrásból származó adatait kombinálhassák.[73] Azt is hangsúlyozza a DMA, hogy a kapuőröknek lehetővé kell tenniük, hogy ha a felhasználó nem járul hozzá az adatok kombinálásához, akkor a végfelhasználónak tájékoztatást kell kapnia arról, hogy a hozzájárulás megtagadása kisebb mértékben személyre szabott ajánlathoz vezethet, egyebekben azonban az alapvető platformszolgáltatás változatlan marad.[74] A DSA ennél is tovább megy, és az online platformot üzemeltető szolgáltatóknak megtiltja, hogy a szolgáltatást igénybe vevők adatait felhasználó, profilalkotáson alapuló hirdetéseket jelenítsenek meg, ha kellő bizonyossággal tudatában vannak annak, hogy a szolgáltatás igénybe vevője kiskorú.[75] A DMA azonban már semmit nem mond arról, hogy mi van akkor, ha a felhasználó a kapuőr szolgáltatását önmagában (adatkumuláció nélkül), személyes adatok átadása nélkül kívánja igénybe venni. A Data Act a nem személyes adatok esetében úgy rendelkezne, hogy a kapuőr nem kérhet és nem kaphat hozzáférést a felhasználóknak valamely termék vagy kapcsolódó szolgáltatás használata vagy virtuális asszisztens által generált adataihoz.[76] Az európai felhasználók többsége azonban kifogásolja, hogy csak személyes adatokért cserébe kap „ingyen" online szolgáltatásokat.[77]

Jay Hoofnagle és Jan Whittington szerint, ha az ingyenesen kínált szolgáltatásokért a cégek pénzt kezdenének el szedni, akkor a magánszféráért aggódók ezeket a szolgáltatásokat reklámok és nyomon követés nélkül élvezhetnék.[78] Marco Botta és Klaus Wiedemann is arra jut, hogy biztosítani kellene a felhasználóknak a választási lehetőséget, hogy a személyre szabott

---

71 Tóth András: A mesterséges intelligencia szabályozásának paradoxonja és egyes jogi vonatkozásainak alapvető kérdései. *Infokommunikáció és Jog,* 2019/2., https://bit.ly/46KlZAe, 3–9.; Communication from the Commission to European Parliament, European Council, the Council, the European Economic and Social Committee, the Committee of the Regions on Artificial Intelligence for Europe, Brussels, 25.4.2018 COM(2018) 237 final, 1.

72 Az MI megbízható működése szempontjából kritikus, hogy az adatok teljes körűek és relevánsak legyenek, különben fennáll az emberi jogok sérülésének veszélye (diszkrimináció, egészség). Lásd White Paper on Artificial Intelligence: A European approach to excellence and trust. European Commission Brussels, 19.2.2020 COM(2020)65 final, 19.

73 N. Moreno Belloso – Nicolas Petit: The EU Digital Markets Act (DMA): A Competition Hand in a Regulatory Glove. *European Law Review,* 2023. április 19., https://bit.ly/3QTBX59, 19.

74 DMA (37) preambulumbekezdés.

75 DSA 28. cikk (2) bekezdés.

76 Proposal for a Regulation of the European Parliament and of the Council on harmonised rules on fair access to and use of data (Data Act), COM/2022/68 final, 36. preambulumbekezdés.

77 Adatvédelmi Eurobarometer 2015, https://bit.ly/47Et1I3.

78 Lásd Chris Jay Hoofnagle – Jan Whittington: „Free: Accounting for the Costs of the Internet's Most Popular Price" 61(3) *UCLA Law Review* (2014) 662.

reklámokért cserébe vagy havi díjért veszik-e igénybe az online „figyelemkereskedők" szolgáltatásait.[79] A brit versenyhatóság tanulmánya is felveti,[80] hogy az online platformoknak biztosítaniuk kellene a felhasználók számára a döntési lehetőséget arról, hogy kívánnak-e személyre szabott reklámokat kapni vagy sem (ez utóbbi esetben csak általános reklámozással szembesülnének). Ennek a választási lehetőségnek a felajánlása az adatokkal való önrendelkezés fényében szükségszerűnek tűnik.

Az adattal fizetés üzleti modelljét ismeri el a szabályozás szintjén a digitális tartalom szolgáltatására és a digitális szolgáltatások nyújtására irányuló szerződések egyes vonatkozásairól szóló uniós irányelv.[81] Az irányelv biztosítékot kínál azokra a szerződésekre, amelyek keretében a kereskedő a fogyasztónak digitális tartalmat szolgáltat, digitális szolgáltatást nyújt vagy erre kötelezettséget vállal, a fogyasztó pedig személyes adatokat ad át, illetve erre kötelezettséget vállal.[82] Bár az irányelv azokra a helyzetekre nem alkalmazandó, amikor a fogyasztó anélkül, hogy szerződést kötött volna a kereskedővel, csak azért kénytelen reklámokat megtekinteni, hogy hozzáférhessen egy digitális tartalomhoz vagy egy digitális szolgáltatáshoz, a tagállamok továbbra is szabadon dönthetnek úgy, hogy kiterjesztik az irányelv alkalmazását az annak hatálya alá nem tartozó ilyen helyzetekre vagy egyébként szabályozzák e helyzeteket.[83] Az irányelv 8. cikk (1) bekezdés b) pontja értelmében a digitális szolgáltatásnak meg kell felelnie a nyilvánosan tett kereskedői kijelentésekből fakadó fogyasztói elvárásoknak. Így tehát egy ingyenes kijelentés azt eredményezi, hogy azért cserébe személyes adat nem kérhető.[84]

Felmerül, hogy a személyes adatok átadásától elzárkózó felhasználónak nyújtott szolgáltatás a továbbiakban maradhat-e ingyenes, megvalósulhat-e pénzbeli fizetési kötelezettség nélkül. Ennek erős indikációi vannak, hiszen az online figyelemkereskedők szolgáltatásai eleve ingyenesen indultak[85] és gyűjtöttek egybe hatalmas felhasználói tömeget. Csak miután dominánssá váltak, akkor emelték meg a reklámok arányát.[86] Jelenleg ugyanis a felhasználók már kétszeresen fizetnek az „ingyenes" szolgáltatásokért: az adataikkal és a figyelmükkel. Bár a célzott reklámok jelentősen növelik az online platformok profitabilitását,[87] indulásuk példája azt mutatja, hogy anélkül is tudnak szolgáltatást nyújtani. Erre figyelemmel az adatvédelmi jog gyakorlásának in-

79 Marco Botta – Klaus Wiedemann: Exploitative Conducts in Digital Markets: Time for a Discussion after the Facebook Decision. 10(8) *Journal of European Competition Law & Practice* (2019), https://doi.org/10.1093/jeclap/lpz064, 475.

80 Online platforms and digital advertising Market study final report. CMA, 2020. július 1., 386–387.

81 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.

82 Uo. (24) preambulumbekezdés.

83 Uo. (25) preambulumbekezdés.

84 Lásd ehhez a Gazdasági Versenyhivatal Facebookkal szembeni elmarasztaló döntését az ingyenesség megtévesztő állítása miatt: https://bit.ly/3QVaEr8.

85 Ráadásul például a Facebook az indulásakor kevesebb reklámot is jelentetett meg, mint az akkor piacvezető versenytárs MySpace, majd csak annak a piacról való kiesése után emelte fel a reklámok arányát a mai – egyes vélemények szerint – kizsákmányoló monopolszintre. Lásd Tim Wu: Blind Spot: The Attention Economy and the Law. *Antitrust Law Journal,* vol. 82., https://bit.ly/3uHJj4z.

86 Uo., 22.

87 Online platforms and digital advertising Market study final report. CMA, 2020. július 1. 44, 42. bekezdés.

gyenesnek kellene lennie abban az értelemben, hogy az adatok átadásától elzárkózás esetén továbbra is díjfizetés nélkül férhessen a szolgáltatásokhoz a felhasználó.

Ez a megoldás abból a szempontból is előnyös, hogy az EU adatvédelmi biztosa szerint az adatvédelmi jog gyakorlása nem lehet a pénzzel fizetés alternatívája.[88] Ha az általános reklámozásból mégsem volna biztosítható a szolgáltatás díjfizetés nélkül, akkor viszont felmerül, hogy be lehet-e vezetni az adattal fizetés mellett a pénzzel való fizetést. Ebben az esetben az adattal fizetés a pénzzel fizetés alternatívája lesz, ami az EU adatvédelmi biztosa szerint ellentétes az adatvédelem szellemiségével, mert a személyes adatok védelme alapvető jog, ezért a személyes adatok nem tekinthetők árunak.[89] Valójában az adattal való fizetés már most is zajlik, de rejtetten, ezért az adatkizsákmányolás melegágya. Ebből következően az adattal való fizetés elismerése éppen az adatvédelem szintjét növelheti, mert biztosítja a választás lehetőségét az adatjogosultak számára, hogy a személyre szabott reklámokat vagy az adataik védelmét tartják-e többre. Főleg, hogy vannak olyan felhasználók, akik pozitívumként értékelik a személyre szabott reklámokat.[90]

Ettől még a személyes adatok átadásának mértékét és intenzitását is szabályozni kellene. Egyrészt azért, mert a figyelemkereskedők piaci hatalma miatt a kizsákmányolásnak nincsen versenypiaci gátja (a fogyasztó nem tud emiatt más szolgáltatóra váltani), másfelől ezt a kizsákmányolást segíti, hogy a felhasználók nincsenek tisztában az átadott személyes adataik valós értékével. Ez utóbbin minden bizonnyal segít, ha a személyes adattal fizető fogyasztók is látják, hogy a szolgáltatásoknak mi a pénzbeli ellenértékük. A személyes adat átadásának mértékét és intenzitását szintén olyan transzparenciát biztosító szabályokkal lehetne kordában tartani, mint amilyen a korábban hivatkozott jól strukturált, lényegre törő adatkezelési tájékoztatás, akár kettős jóváhagyási protokollal, valamint a beleegyezés bizonyos időközönként való megújításának kötelezettségével. Ezen a területen alapvetően a GDPR-t kellene innovatív módon működtetni, különös tekintettel a privacy by design elvre. Lényeges, hogy az olyan felhasználók számára, akik személyes adat átadása fejében veszik igénybe az online szolgáltatásokat, legyen világos, milyen körben és milyen mértékű adatátadást követelnek meg tőlük, hogy tájékozott beleegyezésen alapuló döntést hozhassanak.

A fenti javaslat (az adattal való fizetés lehetőségének megteremtése) egyúttal feloldaná az ún. privacy paradoxot is. A privacy paradox egyfelől arra vezethető vissza, hogy bár a felhasználók aggódnak az adataikért, nem igazán tesznek azok védelméért. Ezen segíthet, ha az adattal fizetés alternatívájaként megjelenő pénzzel fizetés ráirányítja a figyelmet az adatátadás jelentőségére. Másfelől a pénzzel fizetés alternatívája megteremti az adatok erősebb védelmének lehetőségét, így biztosítva, hogy az adatkezelési feltételek megfontolásának valóban legyen tétje.

88 Giovani Buttarelli: *Opinion 4/2017 of the European Data Protection Supervisor,* https://bit.ly/47qKDY0.

89 Uo.

90 Lásd David S. Evans: *The Economics of Attention Markets,* https://bit.ly/49RSy1W, 26–27.; Botta–Wiedemann i. m. (79. lj.) 475.

6. Összegzés

A DMA alapvetően újfajta versenyszabályozás: egyrészt mert konkrét versenyügyek tapasztalatait ülteti át az ex ante jogérvényesítésbe, másrészt mert a digitális piacok támadhatóságát kívánja biztosítani. Ez utóbbi különösen érdekes szabályozáselméleti szempontból. A digitális óriások ugyanis versenyben, ráadásul innovációnak köszönhetően jöttek létre. Ilyen típusú – innovációs versenyt megnyert – piaci hatalmak megregulázása nem gyakori. Maga az innovációs verseny elmélete sem túl régi: a 20. század közepén került a tudományos gondolkodásba, elsősorban Joseph Schumpeter munkásságának köszönhetően. Schumpeter szerint az innovációs piacon a piaci hatalom hosszú távon nem maradhat fenn, mert mindig jöhet új innováció, amely felülmúlja az előzőt. A digitális óriások példájánál azonban felmerül, hogy ez az elmélet esetleg nem állja meg a helyét. Ennek kapcsán számításba kell venni, hogy a digitális óriások komoly erőforrásokat fektettek abba, hogy a rájuk veszélyt jelentő potenciális innovációkat még startup korukban felvásárolják.

Az így kialakult innovációs ökoszisztémák azonban a jövőbeni innovációk szempontjából kulcsfontosságúvá váltak. A DMA célja elsősorban az, hogy ezeket az ökoszisztémákat a potenciális jövőbeli innovációk életképessége szempontjából támadhatóvá tegye. Ennek egyik szabályozási eszköze a digitális piacok adatalapúságát érinti (az adat mint nyersanyag), ami miatt felmerül a DMA és a GDPR kapcsolatának vizsgálata. A DMA a platformok adatgazdálkodását a GDPR-hoz képest is tovább korlátozza. Ennek eszközei:

– az üzleti felhasználók adatainak felhasználási tilalma: ez kifejezetten az aszimmetrikus pozícióból fakad, tisztességtelen gyakorlat, amely az üzletfelek kizsákmányolását és hátrányba hozását eredményezi;

– a személyes adatok kombinálásának megnehezítése: a GDPR-hoz képest a DMA a kapuőrök esetében csak a hozzájárulást ismeri el jogcímként, ha a kapuőrök a felhasználóik különböző forrásokból származó adatait akarja felhasználni vagy összekapcsolni;

– a szolgáltatások személyre szabás nélküli igénybevehetőségnek biztosítása: ez az előző tilalomból fakad, nevezetesen, hogy hozzájárulás hiányában is elérhető legyen a szolgáltatás, ezáltal a kapuőr ne tudja kikényszeríteni a hozzájárulást (ez természetesen nem jelent reklámmenteséget).

A DMA és a GDPR viszonya egy másik szabályozási intézményen keresztül az adathordozhatóság kapcsán is megragadható, amely a GDPR-ban is már egyfajta piaci versenyt előmozdító eszköz, és azt a kapuőrök esetében a DMA tovább áramvonalasítja a folyamatosság és a tágabb adatkezelési jogalapokkal érintett (ráadásul nem csak személyes) adatok irányába. Tehát a DMA versenyszabályozása a szektor adatalapúsága miatt érinti a GDPR-t is, amikor szűkíti a kapuőrök adatokhoz való hozzáférési lehetőségeit, és erősíti a GDPR eleve versenyélénkítőnek szánt adathordozhatósági rendelkezéseit.

Irodalomjegyzék

Apostle, Julia: The EU's Digital Markets Act: What Does It Mean for Businesses and Data Privacy? *Orrick,* 2022. november 1., https://bit.ly/3RbJUUF.

Bania, Konstantina: Fitting the Digital Markets Act in the Existing Legal Framework: The Myth of the „Without Prejudice" Clause. 19(1) *European Competition Journal* (2022) 116–149. https://doi.org/10.1080/17441056.2022.2156730

Belloso, N. Moreno – Petit, Nicolas: The EU Digital Markets Act (DMA): A Competition Hand in a Regulatory Glove. *European Law Review,* 2023. április 19., https://bit.ly/3QTBX59.

Bendiek, Annegret: Integrationspolitische Bedeutung des Digital Service Act (DSA) und Digital Markets Act (DMA). *Stiftung Wissenschaft und Politik,* 2021. március 1., https://bit.ly/47Mc3HC.

Botta, Marco – Wiedemann, Klaus: Exploitative Conducts in Digital Markets: Time for a Discussion after the Facebook Decision. 10(8) *Journal of European Competition Law & Practice* (2019) 465–478. https://doi.org/10.1093/jeclap/lpz064

Bundeskartellamt Prohibits Facebook from Combining User Data from Different Sources, 2019, https://bit.ly/46u3LTI.

Buttarelli, Giovani: *Opinion 4/2017 of the European Data Protection Supervisor,* https://bit.ly/47qKDY0.

Candelon, François – Reeves, Martin: The New Digital World: Hegemony or Harmony? *BCG,* 2017. november 14., https://on.bcg.com/47lK7dI.

Carugati, Christophe: How to implement the self-preferencing ban in the European Union's Digital Markets Act. *Bruegel,* 2022. december 2., https://bit.ly/47LjRct.

Ennis, Sean F. – Evans, Ben: Cloud Portability and Interoperability under the EU Data Act: Dynamism Versus Equivalence. *SSRN,* 2023. március 22., https://bit.ly/3t51yAf.

Evans, David S.: *The Economics of Attention Markets,* https://bit.ly/49RSy1W.

Fleming, Sean: What is Digital Sovereignty and Why is Europe So Interested in it? *World Economic Forum,* 2021. március 15., https://bit.ly/47ogGI3.

Geradin, Damien – Bania, Konstantina – Karanikioti, Theano: *The Interplay between the Digital Markets Act and the General Data Protection Regulation.* 2022, https://bit.ly/3SOPJc5.

Hacker, Philipp – Cordes, Johann – Rochon, Janina: *Regulating Gatekeeper AI and Data: Transparency, Access and Fairness under the DMA, the GDPR and Beyond,* https://bit.ly/3MVNOyy.

Heinemann, Andreas – Meier, Giulia M.: Der Digital Markets Act (DMA): Neues „Plattformrecht" für mehr Wettbewerb in der digitalen Wirtschaft. *Zeitschrift für Europarecht,* 2021, 86–101.

Hennemann, Moritz et al.: *The Data Act Proposal: Literature Review and Critical Analysis, Part I.* Passau, University of Passau, 2023.

Hoofnagle, Chris Jay – Whittington, Jan: „Free: Accounting for the Costs of the Internet's Most Popular Price" 61(3) *UCLA Law Review* (2014) 606–670.

Investigation into Google's 'Privacy Sandbox' browser changes. *Competition and Markets Authority,* 2021. január 8., https://bit.ly/3RcifTP.

Kelber, Ulrich: EU-Digitalstrategie und die dazugehörigen Rechtsakte von DGA, DMA, DSA und AIA – Auswirkungen für den Datenschutz. *Bundesbeauftragten für den Datenschutz und die Informationsfreiheit,* 2022. január 27., https://bit.ly/47O22cH.

Stolton, Samuel: LEAK: Commission in Bid for EU Data Sovereignty with Digital Decade Targets. *Euractive,* 2021. március 8., https://bit.ly/46InNtT.

The World's Most Valuable Resource Is No Longer Oil, but Data. *The Economist,* 2017. május 6., https://econ.st/47rUw7R.

Tóth András: A mesterséges intelligencia szabályozásának paradoxonja és egyes jogi vonatkozásainak alapvető kérdései. *Infokommunikáció és Jog,* 2019/2., 3–9., https://bit.ly/46KlZAe.

VBL-Gegenwert II., Hintergrundinformationen zum Facebook-Verfahren des Bundeskartellamtes, 2017, https://bit.ly/49ILNQh.

Verfahren gegen US-Konzern. EU wirft Amazon Kartellverstöße vor. *Tagesschau,* 2020. november 10, https://bit.ly/3sLqL2z.

Vergnolle, Suzanne: *Enforcement of the DSA and the DMA: What did We Learn from the GDPR?* Hal Open Science, https://bit.ly/49H6bky.

Wils, Wouter P. J.: *The Obligation for the Competition Authorities of the EU Member States to Apply EU Antitrust Law and the Facebook Decision of the Bundeskartellamt.* London, King's College London Law School, 2019.

Witt, Anne C.: The Digital Markets Act: Regulating the Wild West. (60)3 *Common Market Law Review* (2023) 625–666.

Wu, Tim: Blind Spot: The Attention Economy and the Law. *Antitrust Law Journal,* vol. 82., https://bit.ly/3uHJj4z.

Zimmermann, Hendrik – Heinzel, Caroline: Der Digital Markets Act. Plattform-Regulierung für Demokratie und Nachhaltigkeit in der EU–aktueller Stand und Verbesserungspotenziale, *Germanwatch,* 2022. január, https://bit.ly/3GaQogo.