

Doktori (PhD) értekezés tézisei

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

Dr. Tóth Fanni

Témavezető:

Dr. habil. Hajnal Zsolt PhD

egyetemi docens



DEBRECENI EGYETEM

Marton Géza Állam- és Jogtudományok Doktori Iskola

Debrecen, 2026

I. A DOKTORI ÉRTEKEZÉS ELŐZMÉNYEI ÉS CÉLKITŰZÉSEI

Témaválasztásomat motiválta egyrészt az a beszélgetés, amely adott levéltári kutatással összefüggésben bűnügyi személyes adatok nyilvánosságra kerüléséről szólt; másrészt időben egybeesett ez a GDPR 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 EU-ban.

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. Mivel utóbbiak egyúttal fogyasztók is, 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 érintettek, 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.

Az értekezés célkitűzése a személyes adatok kezelésének feltérképezése, ezáltal digitális környezetben az adatvédelem, a versenyjog és a fogyasztóvédelem metszéspontjainak feltárása, a piaci versenyre és a fogyasztókra gyakorolt hatás értelmezése. Egységbe foglaltam azokat az uniós jogforrásokat, amelyek az érintettek védelmén őrködnek a személyes adataik kezelésével összefüggésben. Ennek érdekében részletesen elemeztem a GDPR-t és az elektronikus hírközlési adatvédelmi irányelvet, valamint ez utóbbihoz kapcsolódva vizsgáltam az e-Privacy rendelettervezetet, valamint a digitális omnibusz csomag javaslatának cookie-kra vonatkozó rendelkezéseit. A csomagjavaslat több tekintetben érinti a GDPR rendelkezéseit és a versenyjogi jogszabályokat is, a módosítási javaslatokra röviden utaltam. Elemeztem továbbá a személyes adatok kezelésével összefüggésben a versenyjogi, illetve a fogyasztóvédelmi intézkedéseket tartalmazó jogalkotási aktusokat.

Négy kérdésre kerestem választ, és a következő hipotéziseket fogalmaztam meg:

1.) Tisztában vannak-e a felhasználók a személyes adataik értékével, gazdasági értékkelé válásának folyamatával, valamint 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. 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.*

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? Feltételezésem szerint *a GDPR rendeleti jellege és területi hatálya alapvetően alkalmas az érintettek egységes védelmét biztosítani, 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.*

3.) A személyes adatok kezelése és a piaci verseny összefüggése alapján a GDPR mely rendelkezései váltak további szigorítást motiváló tényezővé, valamint hogy a platformjogszabályokban testet öltő szigorítások milyen irányban képesek befolyásolni a piaci versenyt? 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.*

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

Elsődlegesen a jogszabáylelemző és -összehasonlító módszert alkalmaztam, ehhez alapvető fontosságúnak tekintettem a jogforrások normaszövegét. Értékes forrásnak tekintettem a kapcsolódó uniós dokumentumokat, valamint a vonatkozó nagyszámú szakirodalom eredményeit. Az uniós jogalkotói szándék formálódását a jogszabály-összehasonlító módszerrel vizsgáltam, ami előre- és hátratekintésre is lehetőséget adott. Mind a jogszabáylelemző, mind az összehasonlító módszert alkalmaztam az adatvédelmi, a versenyjogi

és a fogyasztóvédelmi eszközrendszer elemeinek vizsgálatára vonatkozóan. Ez lehetőséget biztosított a jogalkotási aktusok összefüggéseinek átlátására, és annak megállapítására, hogy az uniós lépések mennyire összehangoltak és koherensek. Kisebb mértékben támaszkodtam a történeti módszerre, az adatvédelem fejlődése mozgatórugóinak megállapítása céljából. A jogszabályok gyakorlati szempontú megközelítése érdekében nagyszámú jogesetet vizsgáltam, mind az EUB esetjogából, mind a hazai bírósági és hatósági eljárásokból. Törekedtem arra, hogy a klasszikus példákon kívül az újabbak is fókuszba kerüljenek, és következtetést vonjak le általuk. A jogalkalmazást konkrét példákon keresztül bemutattam megállapításokat az adatvédelem, a versenyjog és a fogyasztóvédelem területén az ellenőrzési, végrehajtási kérdésekre vonatkozóan, valamint az EU jogalkotási folyamatait motiváló tényezőkre.

A dolgozat szerkezeti felépítését tekintve a logika azt kívánta, 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 koncentráltam. Mivel az adatok mindkét jogterület esetében meghatározók, a versenyjogi és a fogyasztóvédelmi szál is átszövi egymást, mégis indokoltnak tartottam külön fejezetben bemutatni ezeket, mert ugyanazt a piaci magatartást más szempontból értékelik és szabályozzák a rendelkezéseik.

II. AZ ÉRTEKEZÉS ÚJ TUDOMÁNYOS EREDMÉNYEI

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 szolgáltatók hogyan jutnak a big data birtokába, azt mire és hogyan használják. A felhasználók gyakran maguk bocsátják rendelkezésre adataikat, más esetben a platformok szerzik meg. 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. A kapott értékek alapján szabják személyre a reklámokat, és célozzák a felhasználókat, így monetizálva a személyes adatokat. Bár a profilalkotás hordozhat

előnyöket, de jellemzően inkább veszélyeket hordoz, mert befolyásolják a felhasználói döntéseket. 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 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 adatgyűjtésén és az adatok monetizálásán alapuló üzleti modelljét, valamint azokat a technológiákat, amelyeket a személyes adatok kezelése során alkalmaznak, 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; az információk vizuális tagolása; a beépített egyszerű választási lehetőségek kínálása; 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 hatékonynak gondolom a

felsorolt megoldásokat, mert már rögzült a beleegyezés-fáradtság. Az információs aszimmetria felszámolásához 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 nem tudják megoldani az aszimmetrikus helyzetet, a platformok nem akarják, a jogalkotók nem vették figyelembe a GDPR megalkotása során az átlagfelhasználótól elvárható informáltságot és magatartást. Ezzel szemben az adatkezelőre vonatkozóan megállapítható, hogy a jogalkotó rengeteg követelményt és szabályt telepít rá, de ha az maximálisan megfelel a GDPR elvárásainak, és ezt bizonyítani is tudja, akkor az adatkezelői pozíció védelme megvalósul, ám 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 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 tolakodó 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 a profilalkotáshoz és a targetált hirdetésekhez kapcsolódóan garanciákat nyújt a jogalkotó (tiltakozáshoz és tájékoztatáshoz való jog), illetve 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 az EDPB-vélemény és a Bizottság vizsgálata alapján sem reális alternatíva. Annak is jelentősége van, hogy a felhasználó tud-e ellene védekezni. Vannak olyan ágazatok, ahol a profilalkotás és a célzott reklámok negatív hatásait képes kivédeni körültekintő, tudatos magatartással. Vannak azonban olyan területek, ahol a reklámok hatása ellen tud, de a profilalkotás következményei ellen nem tud védekezni (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. Az érintetti érdekek megkövetelték a területi hatály kiterjesztését, azaz a tevékenységi hellyel rendelkező és nem rendelkező adatkezelőre is alkalmazni kell, utóbbi esetben nemcsak áruk és/vagy szolgáltatások nyújtásához, hanem viselkedés 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 technológiaselemleges 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. Ennek ellenére nem értek egyet 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 mobil értelmezésű fogalom az érintettre vonatkozóan különböző védelmi szintet jelent majd. Szintén problémaként értékelem azt, hogy az információk értelmezését bizonytalanságot okozó elemek nehezítik. 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, de akár rendszerszintű probléma is. Októl függetlenül mindenképpen alááshatja az érintettek védelmét.

Az érintett személyes adatainak védelme tekintetében a jogszabálytípus, a területi hatály és a fogalmi apparátus alapvető horderejűek, de önmagukban nem elegendőek, 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, az adathordozhatósághoz való jog, az elfeledtetéshez való jog).

Az érintettek védelmét szolgálják az adatkezelő felelősségére épített adatkezelési alapelvek. A célhoz kötöttség, az adattakarékosság, a korlátozott tárolhatóság, a tisztesség, mind hatékony elvek, éppúgy, mint 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, a kockázatok minimálisra csökkentésére. Úgy vélem, hogy a 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 előnyös 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. A nagy ügyek esetében a végrehajtás aránytalan, lassú és nem hatékony. További problémát okoz az, hogy fő felügyelő hatósági szerepet 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. A GDPR eljárási rendelete – 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 kapuórré válás előtt álló vállalkozások okozhatnak újabb, adatkezeléssel összefüggő meglepetéseket, ezzel újratermelve a végrehajtási kérdéseket is. Rendszerszintű végrehajtási problémát hozott felszínre a Facebook

kontra Bundeskartellamt ügy. Az EUB-ítélet szerint, ha 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 szükséges a honlapok működéséhez, más részük a felhasználók személyes jellemzőinek megállapításához visz közelebb. A jelenlegi irányelv nem védi megfelelő szinten a felhasználókat 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 csomag javaslata szerint 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. Technológiásemleges 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, és a platformjogszabályokban testet öltő szigorítások milyen irányban képesek befolyásolni a piaci versenyt?

Az erőfölénnyel való visszaélést vizsgáló és a fúziós ügyek tapasztalatai rámutattak a digitális gazdaságban a személyes adatok kezelése és a piaci verseny alakulása közötti szoros

kapcsolatra. A hatalmas adatvagyon olyan nyersanyagot jelent a platformok számára, amely lehetővé teszi a felhasználói viselkedés elemzését, a felhasználók célzását reklámokkal, kapcsolatépítést az üzleti felhasználókkal stb. A személyes adatok tisztességtelen 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, a piacra gyakorolt hatást a fúziók tovább növelhetik. Ennek ellenére a Bizottság 2017-ig határozottan 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, egyúttal a kisebb vállalkozások segítése, a piacok megmozgatása érdekében a jogalkotónak meg kellett acélosítania a GDPR rendelkezéseit. E célok elérésére legalkalmasabb a jogalapokkal és adathozzáféréssel, -hordozhatósággal kapcsolatos rendelkezések 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 kombinálhatja a személyes adatokat, de nem használhatja fel azokat a nyilvánosan nem elérhető adatokat, amelyek az üzleti felhasználók tevékenységével összefüggésben keletkeznek, vagy amelyeket utóbbiak ügyfelei adtak meg vagy generáltak. A DMA kiterjesztette a GDPR-ban foglalt adathozzáférési és -hordozhatósági jogot is – a végfelhasználók, az üzleti felhasználók és felhatalmazott harmadik felek részére is folyamatos és valós idejű adathozzáférhetőséget biztosít –, ezáltal lehetővé téve a szolgáltatóváltást és az adatoknak a gazdaságba 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, de előtte a személyes adatokat anonimizálni kell.

A GDPR adathozzáférési és -hordozhatósági jogának továbbgondolásából egy teljes rendelet 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 hozzáférhetnek, használhatják és megoszthatják a generált (személyes és nem

személyes) adatokat, 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 kötelezésétől várható nagyobb elmozdulás, ami előhívhatja a felhasználói aktivitást.

Értékelve a platformjogszabályokat, a Data Act korát meghaladó szemlélettel támogatja az adatmegosztást, 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 mennyire lesznek képesek élni a lehetőségekkel, illetve hogy a kedvezményezettek mennyire tudják kiaknázni a rendeletben rejlő potenciált. A Data Acthez viszonyítva a DMA – véleményem szerint – megkésett rendelet, de ebből következő előnye az, hogy ex ante lép fel, és a címzettek körének változását is lehetővé teszi. Ezzel egyenlőbb versenyfeltételeket és tisztességesebb üzleti környezetet teremthet a piacon, és felerősítheti a platformok innovatív erőforrásait. A DMA-t azért tartom megkésettnek, mert a felhasználókra jellemző 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 engedje újratermelni az adatvédelmi problémákat, ami arra enged következtetni, hogy az EU nem védi akaratauk ellenére a felhasználókat, de megteremti számukra a lehetőséget adataik védelmére.

Hipotézisem igazolódott. *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 tehát megerősíteni a platformjogszabályokban, amelyek a platformok tisztességtelen adatkezelése által hozzájárultak a nagy adatvagyonok létrejöttéhez és felhasználásához, 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 az adathordozhatósági jog szintén a DMA-ben és a Data Actben. A platformok adatkezelésének korlátozása és a személyes adatok mobilizálhatósága elősegítheti a piaci versenyt.*

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

Az uniós fogyasztóvédelmi jog úgy igyekszik megerősíteni a fogyasztók védelmét az adataik kezelése tekintetében, hogy a klasszikus szabályozási területek rendelkezéseit egészíti ki. A jogszabályok többsége, ahol ez releváns, a fogyasztó tájékoztatásával, az átláthatóság előírásával kívánja az információs aszimmetriát ellensúlyozni. A CR-irányelv a fogyasztók

többlettájékoztatását írja elő, még a szerződés megkötése előtt, többek között arról, hogy az ár személyre szabott-e. Több, a hirdetések azonosíthatóságát biztosító átláthatósági intézkedést fogalmaz meg a DSA, amelyek a kéretlen hirdetések kontrollálását szolgálják, továbbá az online óriásplatformot és a nagyon népszerű online keresőprogramot üzemeltető szolgáltatóknak a hirdetési adattárukat is nyilvánosan hozzáférhetővé kell tenniük.

A fogyasztóvédelmi eszközrendszer másik elemét a szerződések szabályozása jelenti. A szerződésszerű teljesítésre, a jogorvoslati lehetőségekre stb. vonatkozó jogokat biztosít 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 tárgyalt 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 az érintetti, a 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 kapcsolódnia kell hozzá.

A gyermekeket mint kiszolgáltatott fogyasztói csoportot erőteljesen védi a jogalkotó. A UCP-irányelv 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 – számomra – annak lenyomata, hogy a jogalkotó számára erősebb motivációt jelentett a platformok regulációja, mint a gyermekek érdeke. Véleményem szerint szükséges lenne 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 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 széttöredezettiségéhez vezet az, hogy az egyre szaporodó sötétmegoldás-típusok szabályozási válaszreakciót váltottak ki több jogszabályban is. Kezelésükben a UCP-irányelvre terhelődik a legerőteljesebb szerep, ugyanis ha valamely magatartás nem tartozik a DMA vagy a DSA hatálya alá, akkor megoldást 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. Ez nemcsak további széttöredezettséget, hanem koherenciaproblémákat is felvet, ami az egységes fogyasztói védelem ellen ható tényező. A széttöredezettiség 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 az átláthatatlan technológiák miatt a digitális térben folyamatosan erősödik az aszimmetria, ebből következően az átlagfogyasztó is sérülékenyé válhat; az átlagfogyasztó fogalom mégsem tartalmaz erre vonatkozó elemet. Megoldásként szóba jöhet a UCP-irányelv módosítása, de a jogi normák rendszerszintű technikai beágyazása is, amely a szolgáltatókra terelné 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, 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 azonban 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 stb.) kimutatható párhuzam érvényesül, amelynek középpontjában a fogyasztó védelme áll, kidomborítva azokat az értékeket, amelyek évtizedek óta irányítják a fogyasztók védelmét az EU-ban.

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 sérülékenység kezelésére vonatkozóan még csak körvonalazódnak a jogalkotás szálai. Elengedhetetlenül szükséges lenne tehát a fogyasztóvédelmi jognak gyorsabban és következetesebben reagálni 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 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.*

A személyes adatok kezelésének szerepét vizsgáltam a szolgáltatók és az érintettek, felhasználók kapcsolatában, ami az adatvédelem, a versenyjog és a fogyasztóvédelem szabályozási folyamatait és metszéspontjait is feltárta. Fogyasztóvédelmi adatjogról nem beszélhetünk, az azonban leszögezhető, hogy a digitális környezetre vonatkozóan erősödően van a fogyasztóvédelmi jogszabályokban az adatvédelmi rendelkezések megjelenése, megszilárdítva a fogyasztók jogait. 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 jogalkotási folyamatokkal kapcsolatban azt az álláspontot képviselem, hogy kívánatos lenne, ha a készülő DFA rendelet lenne, horizontális szinten kezelné a digitális sérülékenységet, és illeszkedne az EU digitális szabálykönyvének rendszerébe is. A digitális omnibusz csomag javaslatának nem minden pontjával értek egyet, ezért úgy vélem, egyértelmű határokat kell megállapítani az adatvédelmi célok és az adatok gazdasági hasznosítása céljai tekintetében.

III. AZ ÉRTEKEZÉS TÉMÁJÁBAN SZÜLETETT PUBLIKÁCIÓK LISTÁJA



**DEBRECENI
EGYETEM**

**DEBRECENI EGYETEM
EGYETEMI ÉS NEMZETI KÖNYVTÁR**

H-4002 Debrecen, Egyetem tér 1, Pf.: 400

Tel.: 52/410-443, e-mail: publikaciok@lib.unideb.hu

Nyilvántartási szám: DEENK/228/2026.PL
Tárgy: PhD Publikációs Lista

Jelölt: Tóth Fanni
Doktori Iskola: Marton Géza Állam- és Jogtudományi Doktori Iskola
MTMT azonosító: 10066479

A PhD értekezés alapjául szolgáló közlemények

Folyóiratcikkek, tanulmányok (8)

- Tóth, F.:** The Role of Personal Data and Data Protection in Platform Regulations Affecting Market Competition.
Acta Universitatis Sapientiae Legal Studies. "Accepted by Publisher", 1-15, 2026. ISSN: 2285-6293.
MTA Állam- és Jogtudományi Bizottsága: B
- Tóth, F.:** A személyes adatok és az adatvédelem szerepe a piaci versenyt érintő európai uniós platformjogszabályokban.
Debreceni jogi műhely. 22 (1-2), 205-227, 2025. ISSN: 1787-775X.
DOI: <http://dx.doi.org/10.24169/DJM/2025/3-4/9>
MTA Állam- és Jogtudományi Bizottsága: B
- Tóth, F.:** Az intelligens játékok személyesadat-védelmi vonatkozásai.
Gazdaság és Jog. 31 (11-12.), 48-56, 2023. ISSN: 1217-2464.
MTA Állam- és Jogtudományi Bizottsága: B
- Hajnal, Z., **Tóth, F.:** Protection of Children's Personal Data and Risks Posed by Smart Toys.
Acta Universitatis Sapientiae Legal Studies. 12 (1), 43-59, 2023. ISSN: 2285-6293.
DOI: <http://dx.doi.org/10.47745/AUSLEG.2023.12.1.04>
MTA Állam- és Jogtudományi Bizottsága: B
- Tóth, F.:** A fogyasztó személyes adatai értékének jelentősége.
In: Újratervezés : fogyasztói szabályozási modellek, digitalizáció, adatvédelem. Szerk.: Szikora Veronika, Árva Zsuzsanna, Főnix Média, Debrecen, 157-176, 2019. ISBN: 9789634900795





6. **Tóth, F.:** A GDPR újdonságai: a rendeletjelleg és az érintettek jogai = Novelities of the GDPR ?- the regulation form and the rights of the data subjects.
In: A jog tudománya, a mindennapok joga II. / (szerk.) Siska Katalin, Bodnár Beáta, Győri Ágoston, Ivánka-Tóth Barbara Stella, Joó László Ádám, Kóhalmi Máté, Monok Tamás, Salvador Neto Luis, Szabó Mercédesz Ibolya, Tóth Fanni, Wágner Tamás Zoltán, Debreceni Egyetem, Állam- és Jogtudományi Kar, Debrecen, 126-145, 2019. ISBN: 9789634901242
7. **Tóth, F.:** A GDPR-ról - különös tekintettel a könyvtárakra és levéltárakra.
Debreceni jogi műhely. 15 (1-2), 63-75, 2018. EISSN: 1786-5158.
DOI: <http://dx.doi.org/10.24169/DJM/2018/1-2/8>
MTA Állam- és Jogtudományi Bizottsága: B
8. **Tóth, F.:** Az informatikai bűnözéshez kapcsolódó kényszerintézkedések.
Büntetőjogi szemle. 6 (1), 75-88, 2017. ISSN: 2063-8183.
MTA Állam- és Jogtudományi Bizottsága: C

MTA Állam- és Jogtudományi Bizottsága irányelvei szerint:

„B” kategóriás folyóiratban megjelent publikációk: 5, melyek közül az értekezés alapjául szolgál: 5

„C” kategóriás folyóiratban megjelent publikációk: 1, melyek közül az értekezés alapjául szolgál: 1

A DEENK a Jelölt által a Tudóstérbe feltöltött adatok bibliográfiai és tudományometriai ellenőrzését a tudományos adatbázisok és a Journal Citation Reports Impact Factor lista alapján elvégezte.

Debrecen, 2026.04.27.

