Újratervezés –
fogyasztói szabályozási modellek, digitalizáció, adatvédelem

Szerkesztette:
Szikora Veronika – Árva Zsuzsanna

A Debreceni Egyetem
Állam- és Jogtudományi Karának kiadványa

Felelős kiadó:
Szikora Veronika
dékán
Debreceni Egyetem, Állam- és Jogtudományi Kar

Szerkesztette:
Szikora Veronika – Árva Zsuzsanna

A szövegek korrektúráját
Török Éva
végezte.

A tanulmányokat lektorálták:
Prof. Dr. Bencze Mátyás
egyetemi tanár, tudományos és stratégiai dékánhelyettes
Debreceni Egyetem, Állam- és Jogtudományi Kar
Jogelméleti és Jogszociológiai Tanszék

Prof. Dr. Csécsy György
egyetemi tanár
Debreceni Egyetem, Állam- és Jogtudományi Kar
Polgári Jogi Tanszék

ISBN 978-963-490-079-5

Készült a Főnix Média nyomdaüzemében.

Debrecen, 2019

Újratervezés –
fogyasztói szabályozási modellek, digitalizáció, adatvédelem

Szerkesztette:
Szikora Veronika – Árva Zsuzsanna

A TANULMÁNYKÖTET
AZ IGAZSÁGÜGYI MINISZTÉRIUM
JOGÁSZKÉPZÉS SZÍNVONALÁNAK EMELÉSÉT
CÉLZÓ PROGRAMJAI KERETÉBEN VALÓSULT MEG.

Tartalomjegyzék

Előszó

Az Igazságügyi Minisztérium 2015. november 26-án mutatta be a „Jogászképzés színvonalának emelését célzó programokat", amelynek keretében 2018-ban immár harmadik alkalommal nyílt arra lehetőség, hogy a hazai jogi karok, közte a Debreceni Egyetem Állam- és Jogtudományi Kara az Igazságügyi Minisztérium által támogatott kutatásokat valósítson meg.

2017 nyarán a kutatás- és oktatásfejlesztési támogatások kapcsán új fejezet nyílt, ugyanis a 2016-ban folytatott, jórészt egyéni és egymástól is különböző, sok esetben kevés kapcsolódási pontot tartalmazó téma vizsgálata után, valamennyi jogi kar olyan komplex kutatási témák feldolgozásába kezdett, amely lehetőséget nyújtott egy-egy témakör többirányú megközelítésre, a kutatók széles körének a bevonásával. A Debreceni Egyetem esetében ezt a fő témakört a fogyasztóvédelem jelentette, amelyet egyrészt az indokolt, hogy a kar már több éve aktívan részt vett fogyasztóvédelmi kutatásokban, másrészt a fogyasztóvédelem, mint jogágakon átívelő terület, lehetőséget ad az egyes aspektusok több jogágat is érintő megvizsgálására. Az Igazságügyi Minisztérium támogatása segítségével a korábbi fogyasztóvédelmi kutatásokat aktív műhellyé tudtuk fejleszteni, amelynek keretében intenzív együttműködés jöhetett létre a benne tevékenykedő és az ahhoz kapcsolódó oktatók, PhD-hallgatók és kutatók között.

A 2017-es év után, a jelen kötet alapjául szolgáló 2018-as évben szintén a fogyasztóvédelem témakörében, annak a legújabb dimenzióit vizsgáltuk, amely kutatás a korábbi eredmények alapul vételével és egyes aktuális kérdések megvizsgálásával folytatódott. A 2018. április 1. és 2019. február 28. között zajló kutatás keretében három workshopot és egy zárókonferenciát is szerveztünk, nemzetközi részvétellel. A konferencián a kar több oktatója és kutatója mellett a Cseh Tudományos Akadémia képviselője is előadott, ezzel is megnyitva az utat egy esetleges későbbi nemzetközi összehasonlítás előtt.

A kutatások során olyan, a fogyasztóvédelem aktuális kérdéseit érintő témakörök megvizsgálására nyílt lehetőség, mint *„A fogyasztói jogok védelme a legújabb technológiai vívmányokat hasznosító fogyasztási cikkek használata során"* (alprogram vezetője: Fézer Tamás), *„A hatékony fogyasztói jogérvényesítés új kihívásai a megváltozott társadalmi és piaci környezetben"* (alprogram vezetője: Hajnal Zsolt), *„A belátási képességgel nem vagy részben rendelkező személyek fogyasztói pozícióban"* (alprogram vezetője: Szikora Veronika), *„A jogalkotás eszközei a fogyasztók védelmére"* (alprogram vezetője: Pribula László), *„Pénzügyi fogyasztóvédelem és pénzügyi felügyelet viszonya"* (alprogram vezetője: Horváth M. Tamás), *„Környezetvédelmi közszolgáltatások fogyasztóvédelmi problémái, különös tekintettel a hulladékgazdálkodásra"* (alprogram vezetője: Fodor László), *„Az új közigazgatási eljárás hatása a fogyasztóvédelmi hatósági jogalkalmazásra"* (alprogram vezetője: Árva Zsuzsanna), *„Kellékszavatossági elvek a modern kort megelőző magyar jogban (16-19. század)"* (alprogram vezetője: Szabó Béla), *„A fogyasztói státusz megjelenése az aktuális munkajogi folyamatok között"* (alprogram vezetője: Nádas György). A könyv a fenti kutatócsoportok eredményeit, témacsoportokba rendezve mutatja be.

Az alprogramok egymásra épülve tematikus és koherens rendszerben járták körül többirányú megközelítést alkalmazva a fogyasztóvédelem aktuális polgári jogi, kereskedelmi jogi, peres jogérvényesítést érintő, valamint közigazgatási és munkajogi kérdéseit, amely mellett egy új, eddig nem vizsgált jogtörténeti aspektus is feltárult.

A kutatás eredményeit az oktatásban is hasznosítottuk. 2018 őszén megindítottuk a Debreceni Egyetem által 2017-ben országosan elsőként létesített fogyasztóvédelmi szakjogász képzés első évfolyamát. Az első évében pilot jelleggel indult meg az oktatás nagy szakmai tapasztalattal rendelkező hallgatók részvételével. Ez lehetőséget nyújtott arra, hogy a szakjogász képzésben érdemi visszajelzéseket kapjunk az oktatás továbbfejlesztésére, és a tapasztalatok képzésbe integrálása után tervezzük annak megnyitását más gyakorló szakemberek előtt, ezáltal is a képzés szolgálatába állítva a különböző jogágakban tevékenykedő szakemberek gyakorlati és oktatásfejlesztési tapasztalatait. A képzés iránt eddig is jelentős érdeklődés volt, amely miatt reményeink szerint 2019/2020-as tanévben nagyobb számú részvevőt vonhatunk be hallgatóként, ezzel is lehetőséget kapva arra, hogy a kutatási eredmények nagyobb arányban eljussanak a jogalkalmazókhoz és beépüljenek a joggyakorlatba. Figyelemmel arra, hogy a fogyasztóvédelmi szakjogász képzést a Debreceni Egyetem létesítette, így a jelenlegi szabályok esetén, amennyiben más hazai jogi kar is indítani kívánja a képzést, a Debreceni Egyetem által kidolgozott képzési és kimeneti követelményeket kell követnie, így ezen felelősség tudatában különösen fontosnak érezzük azt, hogy egy olyan stabil szakmai és tudományos alapokkal bíró képzést honosítsunk meg, amely valóban hozzájárulhat a jogászképzés szakmai színvonalának az emeléséhez.

A kutatás eddig elért eredményeit emellett más oktatási területeken is hasznosítjuk, különös tekintettel a fogyasztóvédelmi témájú tantárgyakra, ahol a tananyagba és tematikába integrálva is megjelennek a program által feltárt új területek.

A kutatás eredményeitt összegző tanulmányok két tematikus könyvben jelennek meg:
Újratervezés – fogyasztói szabályozási modellek, digitalizáció, adatvédelem
A fogyasztóvédelmi jogról másképpen – előképek, közjogi és munkajogi vetületek

A kötetek a fogyasztóvédelmi zárókonferencián is bemutatott egyes kutatási eredményeket tartalmazzák, amelyek hangsúlyozottan csak az adott témakörökben folytatott vizsgálatokat tükrözik, azonban korántsem jelentik

a fogyasztóvédelmi komplex kutatás lezárását. Meggyőződésünk szerint a fogyasztóvédelem fiatal és jogágakon átívelő, folyamatosan formálódó, egyre szerteágazóbb terület. Önálló jogággá válását segíthetik elő az olyan kutatások, amelyek minél több szegmensét, annak történeti gyökereit és más jogágakhoz való kapcsolódási pontjait tárják fel, és amelyet a jövőben kiegészíthet egyes problémakörök nemzetközi összehasonlító vizsgálata is.

Szikora Veronika
dékán

Árva Zsuzsanna
dékánhelyettes, IM-kapcsolattartó

Fézer Tamás
egyetemi docens
Debreceni Egyetem, Állam- és Jogtudományi Kar
Polgári Jogi Tanszék

Zoványi Nikolett
adjunktus
Debreceni Egyetem, Állam- és Jogtudományi Kar
Nemzetközi Kommunikációs Szakcsoport

Digitális kényelem kontra a fogyasztók adatainak biztonsága*

Az elmúlt öt év minden korábbi korszaknál dinamikusabb fejlődése az informatikai társadalmi szolgáltatások és technológiák területén olyan hardveres, szoftveres és ezek segítségével indukált kulturális változást, robbanásszerű felhasználóiszám-növekedést eredményezett, mely bár a fogyasztók tartalomfogyasztási igényeire reagálva, mégis proaktív módon növelte meg a fogyasztók adatait potenciálisan fenyegető helyzetek előfordulását, ezzel szinte napi kihívások elé állítva a jogalkalmazókat. Az informatikai iparágban tapasztalható és a XXI. század társadalmára

* A tanulmány az Igazságügyi Minisztérium jogászképzés színvonalának emelését célzó programjai keretében valósult meg.

egyébként is jellemző robotizáció igénye már nem csupán a futurisztikus funkciókkal felruházott készülékek és az azok közötti párbeszéd (*internet of things)* valóságát hozta el relatíve elérhető áron,[1] hanem a mindennapi fogyasztói tevékenységeket támogató kényelmi szolgáltatások piacán is kiélezett versenyt eredményezett. Az informatikai szektorban tevékenykedő vállalkozások világszerte átértelmezték az innováció jelentését, és minden korábbinál nagyobb figyelmet szentelnek az ipari felhasználás mellett a fogyasztói kényelmi szolgáltatások fejlesztésének.[2] A piaci versenyben kialkudott domináns pozíciók ezen vállalkozások számára meglehetősen törékenyek, hiszen a kiélezett versenyhelyzet és a fogyasztók kényelmi szolgáltatások iránti kereslete gyors és kíméletlen átrendeződést eredményezhet a digitális szolgáltatások piacán. A még a 2000-es évek elején is alapvetően a hagyományos értelemben vett számítógéphez (asztali munkaállomások, hordozható számítógépek) kötődő fejlesztések napjainkra egy teljesen más hardverkörnyezetbe tevődtek át; a hordozható eszközök fogyasztói felhasználási szokásokat alapvetően meghatározó primátusa okán egészen sajátos dimenziókat nyitottak meg az informatikai szektor vállalkozásai előtt. A fejlődés különösen az elmúlt néhány évben már korántsem reszponzív. A digitalizáció 1990-es években megindult elterjedése és fejlődése kezdetben és viszonylag sokáig valós felhasználói igényekre és az ipari felhasználók kiszolgálására fókuszált. Az információs társadalmi szolgáltatások ezen sajátossága azonban 2010 után alapjaiban változott meg, amikor az iparág egyértelműen proaktív módon törekszik kielégíteni mesterségesen generált igényeket, méghozzá a fogyasztók és nem az ipari felhasználók szintjén. Az új funkciók, az új szolgáltatások bár mind a fogyasztók kényelmes élet iránti vágyát törekszenek kielégíteni, mégis olyan termékeken keresztül teszik mindezt, melyek sokszor láncszerűen egymásra épülve alakítják ki a fogyasztókban a „kell" attitűdöt.[3]

1 Bővebben lásd: Weber Rolf: Internet of things – Need for a new legal environment, Computer Law & Security Review, 2009/6, 522-527.

2 Bamberge Kenneth A. – Mulligan Deirdre K. – Braman Sandra: Privacy on the Ground: Driving Corporate Behavior in the United States and Europe, The MIT Press (2015) 18.

3 Razaghpanah Abbas – Nithyanand Rishab – Vallina-Rodriguez Narseo – Sundaresan Srikanth – Allman Mark – Kreibich Christian – Gill Phillipa: Apps, Trackers, Privacy, and Regulators A Global Study of the Mobile Tracking Ecosystem, Network and Distributed Systems Security (NDSS) Symposium 2018, San Diego, CA, USA. [Elérhető: http://dx.doi.org/10.14722/ndss.2018.23353 (letöltés dátuma: 2018. december 09.).]

A jogi szabályozás jellemzően jelentős lemaradásban van a személyiségvédelem területén, hiszen általánosan megfogalmazott elveivel, generálklauzuláival, valamint felelősségi rezsimjével egészen 2010-ig egy alapvetően technológiasemleges szabályozás kialakítása mellett kötelezte el magát Európában és az Amerikai Egyesült Államokban egyaránt.[4] Teljesen természetszerű, hogy a személyiség sokszínűsége és a személyiséget alkotó attribútumok, a polgári jogi értelemben vett személyiségi jogok a társadalmi, gazdasági és technológiai változások bűvkörében, számos esetben az adott társadalom kulturális változásainak kitett módon fejlődnek, alakulnak. Ez a folyamat új személyiségi jogok védelem körébe vonását, jogalkotó vagy bíróság általi elismerését és védelemben részesítését, valamint már ismert és nevesített személyiségi jogok új tartalommal való megtöltését eredményezi. Bár a XXI. században számos esetben tapasztalható az európai államok bíróságainak gyakorlatában egyfajta dilemma a személyiségi jogok legteljesebb jogi védelme és a társadalmi együttélés természetes kockázatait viselni köteles fogyasztók egymásnak látszólag ellentmondó koncepcióit érintve, a digitális szolgáltatások piacán mind az Európai Unió jogalkotási szintjén, mind a tagállamokban töretlen az a koncepció, mely a fent említett dinamikus piaci verseny és az abban hallatlan profitra szert tevő multinacionális vállalatbirodalmak jelenléte okán egyértelműen a fogyasztó privátszférájának erős védelme mellett foglal állást.[5] Ezt a szemléletet számos társadalmi, kulturális és pszichés tényező is erősíti. Egyrészről a társadalmi attitűd még mindig sokkal inkább kiszolgáltatott helyzetben lévő szereplőként tekint az egyébként meglehetősen bonyolult és a fogyasztók döntő többsége előtt átláthatatlan programozásra és hardveres hátteret igénylő szolgáltatások technológiai megvalósítására, másrészről pedig a hordozható informatikai eszközök népszerűsége és elterjedése megsokszorozta a jogsértéses helyzetek előfordulásának lehetőségét. Napjainkban a tranzakciók klasszikus és ősi ellenértéke, a pénz mellett a digitális szolgáltatások piacán lassan a pénzzel azonos pozíciót követel magának a fogyasztó adatainak köre, mely valós ellenértékként funkcionál számos helyzetben, adatért kínálva újabb és újabb kényelmi szolgáltatásokat

4 Bamberg et al.: i. m. 26.

5 Voss W. Gregory – Woodcock Katherine H.: Navigating EU Privacy and Data Protection Laws, American Bar Association (2016) 56.

a jogosult számára. Nem tagadhatjuk azonban, hogy az adat mint pénz jelenség gyakorlatilag pontosan a pénzen alapuló profitszerzés előszobája, illetve legújabb módszere, hiszen az adatok alapján, prediktív algoritmusokat használó elemzésekkel olyan célzott marketingtevékenység fejthető ki, mely a fogyasztót már ténylegesen pénzfizetést igénylő tranzakciók megkötésére sarkallhatja.[6]

Az adatvédelmi jog közjogi és magánjogi garanciái a 2010-es évekig alapvetően technológia-semleges szabályozási koncepciót követő európai jogi rezsimben hatástalannak bizonyulnak a digitális kényelmi szolgáltatások piacán, hiszen a klasszikus és még mindig inkább offline jogsértési környezetre modellezett védelmi mechanizmusok gyakran idegesítő beavatkozást igényelnek a fogyasztó oldalán, mintsem tudatos választásokra, beállítások alkalmazására sarkallnák őt. Jó példa erre a weboldalak látogatásához kapcsolódó, a fogyasztó adott honlapon kifejtett tevékenységét (pl. keresési és találati érdeklődés, korábbi vásárlások, hozzászólások, feltöltött vélemények, értékelések stb.) naplózó, úgynevezett *cookie* jog jelenleg is alkalmazott, a fogyasztó hozzájárulását követelő előírása[7], mely minden újabb weboldal meglátogatása során felugró ablakok, a honlapon elérhető tartalom olvashatóságát korlátozó sávok (*banner*ek) formájában kér hozzájárulást a fogyasztótól ezen adatok gyűjtéséhez, tárolásához és elemzéséhez. Ez az alapvetően garanciálisnak szánt rendelkezés az európai adatvédelmi jogban a legtöbb fogyasztót automatikus kattintásokra sarkallja, hiszen a digitális kényelmi szolgáltatások fogyasztó számára vonzó célkitűzéseivel éppen ellentétesen hat: a böngészés és általában a digitális tartalomfogyasztás és tartalomlétrehozás élményét rontja, idegesítő akadályokat gördítve a tevékenység végzése elé.[8]

Jelen tanulmány célja annak bizonyítása, hogy különösen az egyelőre definíció szintjén is nehezen megfogható digitális kényelmi szolgáltatások adatvédelmi vonatkozásai körében a technológia-semleges szabályozás talán minden más

6 Bamberg et al.: i. m. 73.

7 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), Official Journal L 201, 31/07/2002. 0037-0047.

8 Markou Christina: Behavioural advertising and the new 'EU Cookie Law' as a victim of business resistance and a lack of official determination, Springer (2016) 33.

jogterülethez képest szembetűnőbb módon tarthatatlan és hatástalan. Ezen hipotézis alátámasztására néhány, napjaink forró témajaként emlegetett digitális kényelmi szolgáltatás elemzésén keresztül mutatjuk be, hogy az Európai Unióban jelenleg hatályba lévő e-Privacy vagy hivatalos nevén elektronikus hírközlési adatvédelmi irányelv rendelkezései és az ezek nyomán kialakult védelmi mechanizmusok milyen veszélyeztetett területeket hagynak figyelmen kívül, illetve az egyébként a szabályozás értelmét adó, az irányelv megalkotásakor is ismert szolgáltatások fogyasztók általi igénybevétele során milyen hatásfokot rontó tényezőkkel szembesülnek. Az elemzés a folyamatosan mozgásban lévő digitális kényelmi szolgáltatások piacának sajátosságai miatt nem lehet teljes körű, így nem fedhet le valamennyi, akárcsak a tanulmány megírásának pillanatában létező és a fogyasztók széles köre előtt ismert szolgáltatást, ahogyan generális megállapításokat sem tehet a jövőbeni szabályozás kialakítására, pontosan a fent említett technológia-semlegesség elméletének megdőlése okán. Bevallott célunk azonban, hogy az Európai Unió égisze alatt éppen készülő és a jelenleg hatályos e-Privacy irányelvet remélhetőleg hamarosan felváltó e-Privacy rendelet megalkotása során[9] ráirányítsa a figyelmet néhány szabályozási lehetőségre.

1. A digitális kényelmi szolgáltatások jelentése, fajtái

A digitális kényelmi szolgáltatások olyan szerteágazó szolgáltatásokat foglalnak magukban, melyek akár hardveres, akár szoftveres formában kínálnak a fogyasztók mindennapi tevékenységét megkönnyítő megoldásokat, és melyek ezen megoldások megvalósítása érdekében a fogyasztó személyes adatait felhasználják. E szolgáltatások közé sorolhatók a termékek és szolgáltatások ellenértékének kiegyenlítését segítő szolgáltatások, melyek jellemzően alkalmazásba integrált online fizetéseket, fizetési megbízások online feladásának lehetőségét kínálják, és mindkét területhez kapcsolódóan biometrikus azonosítók felhasználását igénylik.[10] Ideérthetők továbbá azok

9 Javaslat az Európai Parlament és a Tanács Rendelete az elektronikus hírközlés során a magánélet tiszteletben tartásáról és a személyes adatok védelméről, valamint a 2002/58/EK irányelv hatályon kívül helyezéséről (elektronikus hírközlési adatvédelmi rendelet), 2017. január 10., COM(2017) 10, 2017/0003(COD).

10 Sammons John: The basics of digital forensics: The primer for getting started in digital forensics,

a szolgáltatások is, melyek a felhasználói profilhoz kötött adattárolás lehetőségét kínálják, és e körben sokszor korlátozott fogyasztói kör számára hozzáférhető tartalmak megtekintése előtti azonosításhoz használnak jellemzően születési időhöz, lakcímhez kapcsolódó adatokat. Napjaink talán legtöbb vitát kiváltó digitális kényelmi szolgáltatása azonban kétségtelenül a lokalizációs szolgáltatások alkalmazása.[11] A lokalizációs szolgáltatások a fogyasztó tartózkodási helye alapján szűrnek digitális tartalmakat annak érdekében, hogy a lehető legspeciálisabb és legrelevánsabb ajánlatokkal, illetve információkkal segítsék a fogyasztót mindennapi szükségletei kielégítésében. E körben példát jelenthetnek az éttermeket listázó alkalmazások, az utazási szolgáltatásokat kínáló alkalmazások, de ugyanígy lokalizációs adatokon alapulnak fitness és egészségalkalmazások is. A fogyasztó számára a kényelem a fizetések gyors és a fogyasztó oldalán szinte semmilyen hosszútávú memóriát nem igénylő megoldásaiban, a releváns tartalomhoz való gyors hozzáférésben, valamint a specializált információszolgáltatásban keresendő, ugyanakkor minden itt példaként felhozott szolgáltatás közös attribútuma, hogy olyan személyes adatok adják a szolgáltatás működésének alapját, melyek a fogyasztót egyedileg azonosíthatják. Ez az egyedileg azonosíthatóság adja egyben a kényelmi szolgáltatások legnagyobb veszélyforrását is. Az azonosítás a még az ezredforduló után is hosszú ideig uralkodó felhasználónév-jelszópáros vagy éppen kódok és többcsatornás azonosítási megoldások helyett jellemzően biometrikus adatokon alapul. A fogyasztó ujjlenyomata, íriszképe, illetve arca az, amely a szolgáltatásokba való belépést, az általuk kínált tevékenységeket autorizálja. Tekintettel arra, hogy ezek a biometrikus azonosítók mindig a fogyasztónál vannak, és olyan egyedi tulajdonságait jelenítik meg a fogyasztónak, mely szinte kizárja az azonosítási hiba lehetőségét, a kényelmi szolgáltatások körében egy jelentős szintlépést eredményezett.

A biometrikus azonosítás előszobája azonban a hordozható eszközök elterjedése és a rajtuk tárolt, segítségükkel megosztott információk körének kiteljesedésében keresendő. A mobileszközök bár napjainkban is alapvetően az okostelefonok köré épülnek, az elmúlt néhány évben a

Syngress (2014) 31.

11 Razaghpanah et al.: i. m.

viselhető eszközök (*wearables)* irányába is jelentős elmozdulás történt. Az okosórák, okosszemüvegek, okoskarkötők világában az ember leglényegibb, legszemélyesebb információival állandó és szoros kapcsolatban lévő eszközök segítségével a kényelem könnyen maximalizálható. Ezek a hordozható eszközök a rendkívül fejlett biometrikus azonosítás segítségével az adatbiztonság sokszor fals képzetét keltik a fogyasztóban, hiszen az eladhatóságuk növelése érdekében alkalmazott reklámkampányok mind a más fogyasztóktól mint illetéktelen személyektől való védelem tökéletes megoldásaiként tekintenek ezekre a médiumokra. A fogyasztók ezen fals adatbiztonságba vetett hitben tárolnak a privátszféra körébe értett egyre személyesebb és egyre érzékenyebb adatokat és információkat, melyek egy mobiltelefonon tárolt és megosztott tartalom akár rövid ideig tartó elemzésével is szinte teljes személyiségprofil meghatározására kínálnak lehetőséget. A biometrikus azonosítás ugyan a legtöbb esetben – természetesen az alkalmazott technológia függvényében – valóban képes magas fokú biztonságot nyújtani az eszközön tárolt és annak segítségével megosztott adatok vonatkozásában, azonban a fogyasztók számára sokszor nem nyilvánvaló veszélyforrásként jelen van az alkalmazást üzemeltető vállalkozás, illetve sok esetben maga a hardvergyártó is képes hozzáférni az eszközön tárolt tartalmakhoz.[12] Társadalmunk sajátossága, hogy a nagy nemzetközi cégbirodalmakba vetett bizalom felülírja a fogyasztók döntő többségének gyanakvását, és csupán a másik fogyasztótól való félelem, az előle való eltitkolás motivációja az, amely vásárlásra ösztönöz. A digitális kényelmi szolgáltatások ezáltal a kényelmen túl a kelendőségük növelése érdekében alkalmazott szuperbiztonságosnak tűnő azonosítás lehetőségét is kínálják.

Számos európai uniós tagállami bíróság gyakorlata elfogadta azt az álláspontot, miszerint ezeken a mobileszközökön tárolt adatok a fogyasztó privátszférájába vonhatók, így például egy okostelefonhoz történő illetéktelen hozzáférés szinte automatikusan személyiségi jogi jogsértést valósít meg, a hozzáféréssel érintett adatok természetétől függetlenül. A hordozható eszközök, melyek lényegében maguk is kényelmi szolgáltatások, az ember privátszférájának

12 Voss W. Gregory – Woodcock Katherine H.: Navigating EU Privacy and Data Protection Laws, American Bar Association (2016) 111.

manifesztálódott megjelenései, így olyan személyes használati tárgyakat jelentenek, melyek a külvilág elől rejtve kell, hogy maradjanak.[13]

Bár a definícióalkotás meglehetősen nehézkes a digitális kényelmi szolgáltatások vonatkozásában, tekintettel arra, hogy a diverz technológiai megoldásokat alkalmazó vállalkozások termékei és szolgáltatásai nehezen kategorizálhatók, azonban közös attribútumként mégis kiemelhető e szolgáltatások személyes adatokat felhasználó volta. A jogi szabályozás szempontjából éppen az adatvédelmi incidensek lehetőségét magukban hordozó jellemzőik miatt kerülhetnek az érdeklődés középpontjába ezek a szolgáltatások, azonban kérdéses, hogy az Európai Unió egyébként meglehetősen koherens és szofisztikált adatvédelmi rezsimjébe, melyet elsődlegesen az Általános Adatvédelmi Rendelet (a továbbiakban: GDPR)[14] jelenít meg, mennyiben illeszthetők bele a digitális kényelmi szolgáltatások. Véleményünk szerint a GDPR alapelveit alkalmazva konkrét jogsértéses helyzetekben talán minden alkalommal meghatározható a felelősség alanya és köre, azonban az európai fogyasztóvédelmi szemlélet alapvetően preventív felfogása nem feltétlenül ezt a *post-event* megközelítést támogatja. Álláspontunk szerint a közjogi szabályozás és a magánjogi védelmi rezsim kölcsönhatásában léteznie kell olyan technológia-specifikus előírásoknak, melyek egyrészről a fogyasztót olyan információs és rendelkezési helyzetbe hozzák, ahol megalapozott döntést tud hozni egy digitális kényelmi szolgáltatás használatával, használati körével kapcsolatban, másrészről szelekciót engednek a fogyasztókért folytatott piaci versenyben a szolgáltatást igénybe vevők számára. Ez utóbbi célkitűzés akkor valósul meg, ha a fogyasztók a kötelezően rendelkezésükre bocsátott információk birtokában nem csupán alkalmazások, termékek, hanem az azok mögött megjelenő szolgáltató és gyártó vállalkozások egészére vonatkozóan tudnak következtetéseket levonni az adatbiztonság szempontjából értékelt megbízhatóságukat, kereskedelmi szavahihetőségüket illetően.

13 Ibid. 134.

14 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), Official Journal L 119, 4.5.2016, 1-88.

2. A jogi szabályozás személyi és tárgyi hatálya

Az európai uniós adatvédelmi rezsimre úgy tekintünk, mint egy közjogi és magánjogi szabályozók együttműködésén alapuló, kötelezéseket, kollektív és individuális kikényszerítési mechanizmusokat egyaránt tartalmazó és kínáló rendszerre, amely prevenciós és *post-event* reparációs/kompenzációs célokat egyaránt képes kiszolgálni. Az információs társadalommal összefüggő szolgáltatások piacán azonban a prevenció és a reparáció egyensúlya szükségképpen felborul. Az adatvédelmi incidensek következtében a fogyasztónál előállt hátrányok kompenzálására hivatott intézmények ugyanis pontosan a digitális környezet kínálta anonimitás, relatív törölhetetlenség és tömegek számára biztosított gyors és olcsó hozzáférés miatt még megközelítőleg sem képesek feltétlenül az okozott sérelmeket enyhíteni.[15] Amennyiben a polgári jogi személyiségvédelem kontinentális hagyományokon alapuló, vétkességtől független és vétkességi alapú dualista szankciórendszerét vesszük alapul, még a két eszköztár kombinálása sem biztosíthat megfelelő kompenzációt és elégtételt a sérelmet szenvedett fél számára. A jogsértő vétkességétől – magyar fogalmaink szerinti felróhatóságától – független személyiségvédelmi eszközök (pl. jogsértés abbahagyására kötelezés, jogsértéssel előállt tárgyak megsemmisítése, a jogsértéssel elért vagyoni előny kiadása stb.) is alacsony hatásfokúak lehetnek, hiszen a jogsértés körülményeinek feltárása, ezáltal a jogsértéssel okozott hátrányok köre és terjedelme is komoly nehézségekbe ütközik. Annak megállapítása, hogy a digitális kényelmi szolgáltatások használata során jogellenesen megszerzett, fogyasztói személyes adatok milyen körben és milyen célból kerültek felhasználásra, a digitális közeg sajátosságai okán szinte követhetetlen, és számos esetben a szolgáltatás üzemeltetőjének önbevallásán alapulva bizonyítható, meglehetősen kétes eredményt kínálva. A vétkességtől – felróhatóságtól – függő szankciók körében előkelő helyet elfoglaló, a jogsértővel szemben vagyoni hátrány kilátásba helyezését kínáló kártérítés/sérelemdíj követelésének lehetősége pedig különösen a csoportkereseteket (*class action)* nem ismerő kontinentális jogrendszerekben elhanyagolható preventív és exemplifikatív erővel bír a gyakran kötelezetti oldalon megjelenő nemzetközi cégbirodalmak számára. A közjogi szankciók –

15 Martinez Dolores-Fuensanta: Unification of personal data protection in the European Union: Challenges and Implications. [Elérhető: http://www.elprofesionaldelainformacion.com/contenidos/2018/ene/17_esp.pdf (letöltés dátuma: 2018. december 10.).]

jellemzően közigazgatási bírságok – már nagyobb preventív hatást fejthetnek ki, különösen a GDPR hatályos bírságolási rendszerét[16] alapul véve, ahol a jogsértő vállalkozás gazdasági teljesítménye – éves árbevétele – képezi a bírságszámítás alapját. A közjogi szankciók esetében ugyanakkor számolnunk kell a látens jogsértések nagy számával, hiszen a tipikusan tagállami adatvédelmi hatóságok és intézmények komoly infrastrukturális lemaradásban vannak a digitális kényelmi szolgáltatások globális színterén tevékenykedő és a jogsértéseket megvalósító vállalkozásokkal szemben. Egy-egy adatvédelmi incidensről és jogsértő gyakorlatról való tudomásszerzés is nehézkes, de még a tudomásszerzést követően is rendkívüli nehézséget jelent az eljárás lefolytatása, a jogsértés bizonyítása. E körben valódi visszatartó erő a vállalkozások szempontjából a dinamikus és kiélezett gazdasági verseny, amelynek keretei között az egymással versengő piaci szereplők egymás jogsértéseit leplezik le és hozzák nyilvánosságra, a fogyasztói bizalom erősítése és az irántuk való piaci szimpátia növelése érdekében.[17] Még azonban ennek a hatásfokát is rontja a gyakran tapasztalható, óriásvállalatok közötti együttműködés, ahol a vállalatok tulajdonképpen egymás partnerei az adatvédelmi jogsértések megvalósítása során (pl. az egyik vállalkozás a másik részére értékesít, ad át személyes adatokat ellenérték fejében).

Az adatvédelmi szabályozás számos szolgáltatót engedélyezési, bejelentési, nyilvántartási kötelezettség alá von, azonban ezen vállalkozások köre még mindig csekély ahhoz képest, hogy hány és milyen tevékenységet folytató vállalkozás valósíthat meg adatvédelmi jogsértést a kényelmi szolgáltatások nyújtásán keresztül. Az internet-szolgáltatók klasszikusan engedélyezés alá eső vállalkozások, akiknek a gazdasági tevékenységét komoly figyelem kíséri a tagállami hatóságok részéről. Az internet-szolgáltatók rendszerein továbbított adatok és közvetített tartalmak monitorozása azonban sem az európai, sem az USA jogrendjében sem automatikus kötelezettsége ezeknek a szolgáltatóknak. Mind az Európai Unió, mind az Egyesült Államok az úgynevezett *notice and take down* eljárást és hozzáállást követi ezzel kapcsolatban, azaz az internet-szolgáltatóknak nem kell konkrét preventív lépéseket tenniük az infrastruktúrájukat használó tartalom ellenőrzése terén,

16 Általános adatvédelmi rendelet, 83. cikk.

17 Solove Daniel J. – Schwartz Paul M.: Information Privacy Law, Aspen Publishers (2017) 65.

pusztán a tudomásukra jutott jogsértésekre kell reagálniuk azzal, hogy a jogsértő tartalmat blokkolják.[18]

Az online fizetési szolgáltatások egy jelentős része, mely alapvetően a direkt bankkártyás fizetésekre épít, egy pénzforgalmi szolgáltató által működtetett és fejlesztett rendszeren keresztül bonyolódik. Számos kártyakibocsátó szolgáltató maga is kínál a fogyasztó számára olyan, a hordozható eszközeire telepíthető alkalmazásokat, melyek segítségével letárolhatók a kártyaadatok, és közvetlenül az alkalmazásból indíthatók fizetési műveletek. A pénzforgalmi szolgáltatók engedélyezési és szigorú monitorozási eljárások hatálya alatt állnak Unió szerte, és ezeknek a közjogi szabályzók által meghatározott eljárásoknak egyik sarkalatos pontját képezik az adatvédelmi kötelezések, valamint azok megtartására irányuló ellenőrzési eszközök. A pénzforgalmi szolgáltatók maguk is több esetben kötnek szerződést a fogyasztók körében népszerű hordozható eszközöket gyártó vagy éppen népszerű alkalmazásokat üzemeltető vállalkozásokkal annak érdekében, hogy a digitális kényelmi szolgáltatások piacán ők és fizetési eszközeik is megjelenhessenek (pl. az Apple Pay technológia az Apple és a pénzforgalmi szolgáltatók megállapodásán alapuló fizetési megoldás, mely biometrikus azonosítás segítségével, előre letárolt kártyákat használva kínálja az érintésmentes offline és az online fizetés lehetőségét). Tekintettel arra, hogy az ilyen együttműködések, szerződéses konstrukciók a pénzforgalmi szolgáltató jelenléte okán továbbra is megtartják a pénzforgalmi szolgáltatókra egyébként irányadó adatvédelmi előírásokat, titkosítással kapcsolatos kötelezéseket, jellemzően nem vagy csupán csekély mértékben jelentenek veszélyt a fogyasztók személyes adataira nézve. Egyre növekvő számban vannak azonban jelen azok az alkalmazások és szolgáltatások, melyek a fogyasztó önkéntes hozzájárulásán alapulva tárolják le a bankkártya adatokat, majd az alkalmazás segítségével összekapcsolódó szerződő felek (jellemzően a vállalkozás és a fogyasztó) között az ellenérték megfizetésének platformját adják (pl. PayPal, WePay, 2Checkout, Dwolla, Stripe, Worldpay stb.). Ezek a fizetési platformok már jellemzően nem minősülnek pénzforgalmi szolgáltatóknak, hiszen a fizetési tranzakciók megvalósítása során úgynevezett ráépülő szolgáltatásként csupán háttérinfrastruktúrát biztosítanak a szerződő

18 Voss et al.: i. m. 156.

felek számára, fizetési eszközöket azonban nem bocsátanak ki és nem hoznak létre. A fizetési platformokra így a pénzforgalmi szolgáltatókra irányadó engedélyezési, ellenőrzési, felügyeleti előírások nem vonatkoznak, és adatvédelmi kötelezések szempontjából csupán a valamennyi vállalkozásra irányadó, általános adatvédelmi kötelezettségek terhelik őket.[19]

A GDPR személyi hatálya az Európai Unióban bár valamennyi, természetes személyek személyes adatai bármilyen formában kezelő vagy feldolgozó vállalkozásra kiterjed[20], a speciális, kifejezetten a digitális térben létező adatkezelésekre és adatfeldolgozásokra vonatkozó különös kötelezettségek hiányában javarészt alapelvi jelleggel és nem az adott technológiára specializálva találhatunk kötelezettségeket az adatvédelem eszméjének érvényre juttatása körében. Hangsúlyozzuk, hogy individuális igényérvényesítések vagy kollektív jogérvényesítés keretében indult jogvitákban a GDPR általános szabályainak és alapelveinek alkalmazásával is vélhetően eljuthatunk az adatvédelmi jogsértések megállapításához, akár a legsajátosabb és leginnovatívabb digitális kényelmi szolgáltatás vonatkozásában is, azonban az adott technológiára, szolgáltatásra specializált különös előírások hiányában a prevenció jellemzően nem valósul meg. Ezek a vállalkozások ugyanis az általuk alkalmazott technológiára individualizált adatvédelmi kötelezettségek hiányában szinte kizárólag a piaci verseny által diktált tényezők hatására döntenek adatvédelmi rendszerek kidolgozása, alkalmazása mellett vagy éppen negligálják az ilyen technológiák beemelését saját szolgáltatásaikba.

A fenti okfejtés mentén látható, hogy a digitális kényelmi szolgáltatások nyújtói vonatkozásában az adatvédelmi szabályozás közjogi oldala meglehetősen hiányos, és specializált előírások nélkül a preventív célokat nem képes megvalósítani. Az adatvédelemi magánjogi személyiségvédelem körében értékelt megjelenése oldaláról vizsgálva a problémát ismét azt láthatjuk, hogy a személyiségi jogi katalógus kiterjesztése a digitális énképek és a digitális térben megjelenő információk, gondolatok, személyes adatok tekintetében bár nem okozott problémát a tagállami bíróságoknak és bizonyos tagállamokban

19 Leenes Ronald – van Brakel Rosamunde – Gutwirth Serge – De Hert Paul (szerk.): Data Protection and Privacy: The Internet of Bodies, Hart Publishing (2018) 94.

20 Általános adatvédelmi rendelet, 4. cikk 18. pont.

a jogalkotónak sem, azonban a személyiségvédelmi szabályozás sajátos rendszeréből következően itt is túlzottan generális szabályokkal találjuk magunkat szemben. A polgári jogi személyiségvédelem alapvetően deklaratív és reaktív hatású intézményrendszer. A deklaratív funkció megjelenése abban érhető tetten, hogy a személyiségi jogok általános védelembe vonása és a személyiségvédelmi igények abszolút szerkezetű jogviszonyok keretei között történő felfogása egy magatartási mintát kíván kínálni a polgári jog alanyainak. A deklaráció azonban nagyon kevés esetben és igen kevés személyiségi jog esetében vállalja fel a definícióalkotást valamely személyiségi jog vonatkozásában. Abból kiindulva, hogy a személyiségi jogok jellemzően maguk is a társadalmi, gazdasági és technológiai fejlődés és változások által alakulnak, formálódnak, statikus definíciók még ernyőfogalmak szintjén sem alkothatók. A digitális önrendelkezési jog az információs önrendelkezési jog egy sajátos szeletét adja, amely az információs társadalommal összefüggő szolgáltatások kategorizálhatatlansága okán jellemzően nem ölt kodifikált formát. A deklaráció így az adatvédelmi ernyőszabályokba beleértett módon jelenik meg vonatkozásában. A személyiségvédelem reaktív természete abban érhető tetten, ahogyan a magánjog rendszerének helyreállítást célzó koncepciójába illeszkedően személyiségvédelmi eszközök tárházát vonultatja fel, jogorvoslatot kínálva a személyiségi jogok megsértésének esetére. A szankciórendszer azonban megtörtént jogsértések következményeit hivatott enyhíteni, megközelítőleg kiküszöbölni, preventív célokat azonban legfeljebb a polgári jogi felelősségben mindig jelenlévő prevenciós szemléleten keresztül, meglehetősen alacsony hatásfokkal tud megjeleníteni. A digitális kényelmi szolgáltatások és az azokon keresztül hozzáférhető személyes adatok vonatkozásában így konkrét jogsértési helyzeteket, konkrét, a szolgáltatót terhelő kötelezettségeket éppen úgy nem tartalmaz a magánjog, mint ahogyan a közjog sem.[21]

21 Rotenberg Marc: Privacy Law Sourcebook 2018, Amazon Digital Services LLC (2018) 123.

3. Digitális kényelmi szolgáltatások és az európai adatvédelmi szabályozás nyújtotta garanciák

Jogszerű célra, az EU jog lehetővé teszi, hogy szigorú és egyértelműen meghatározott feltételek mellett a szolgáltatók bizonyos információkat gyűjtsenek a fogyasztók digitális térben végzett cselekményeivel kapcsolatban.[22] E körbe vonható például a lokalizációs adatok gyűjtése és más formában történő kezelése. Az EU adatvédelmi rezsimje azonban kifejezetten tiltja az ilyen adatok céltól eltérő felhasználását, ezen cselekményeket a privátszféra megsértésének körébe értve. Az EU Alapjogi Charta[23] a 2009-es Lisszaboni Szerződéstől kezdődően elsődleges jogként funkcionál az Unió jogrendszerében, és a Szerződésekkel azonos hatállyal határoz meg kötelezettségeket a tagállamok számára.[24] A Charta 7. és 8. cikkei elismerik és garantálják a magán- és családi élet, valamint a személyes adatok védelmét. A 8. cikk (2) bekezdése kifejezetten előírja, hogy az érintett jogosult hozzáférni és kijavítását kérni a róla gyűjtött személyes adatoknak, és ez a jogszabályhely teszi lehetővé azt is, hogy az érintett beleegyezésével róla tisztességes és meghatározott célból, illetve jogszabály által megengedett célból adatot kezeljenek. Az Európai Unió Bírósága 2014. április 8-án érvénytelenítette az adatmegőrzési irányelvet.[25] Az érvénytelenítés egyik indoka éppen az Alapjogi Charta 7. és 8. cikkében garantált jogok megsértése volt.[26] Az adatmegőrzési irányelv témánk szempontjából azért bír jelentőséggel, mert a digitális kényelmi szolgáltatások esetében az egyik legtöbbet kezelt adat, a lokalizációs adatok vonatkozásában az irányelv rendelkezései kifejezetten megengedték, hogy a mobil applikációk üzemeltetői ezeket az adatokat megőrizzék.[27]

22 Elektronikus hírközlési adatvédelmi irányelv, 9. cikk.

23 Az Európai Unió Alapjogi Chartája, Official Journal, 2012/C 326/02.

24 Az Európai Unió Működéséről Szóló Szerződés (EUMSZ), 6. cikk.

25 Az Európai Parlament és a Tanács 2006/24/EK irányelve (2006. március 15.) a nyilvánosan elérhető elektronikus hírközlési szolgáltatások nyújtása, illetve a nyilvános hírközlő hálózatok szolgáltatása keretében előállított vagy feldolgozott adatok megőrzéséről és a 2002/58/EK irányelv módosításáról (adatmegőrzési irányelv), Official Journal L 105, 13.4.2006, 54-63.

26 Digital Rights Ireland Ltd. v. Minister for Communications, Marine and Natural Resources (C–293/12).

27 Adatmegőrzési irányelv, 3. cikk.

Az Európai Emberi Jogi Egyezmény is elismeri a magánélethez fűződő jogot, mely magában foglalja az internetet használók privátszférájának védelmét is.[28] Az Emberi Jogok Európai Bírósága (a továbbiakban: EJEB) gyakorlatában az Egyezményben biztosított alapvető szabadságok és jogok digitális környezetben történő megsértése nyomán születő igények elbírálása is a Bíróság hatáskörébe tartozik.[29] Az EU Alapjogi Charta és az Emberi Jogok Európai Egyezményének hatálya alatt tehát nincs jelentősége annak, hogy az ezen dokumentumokban garantált jogok megsértését, azaz a privátszférába való betüremkedést milyen vállalkozás vagy entitás valósította meg, azaz a magánéletet érintő fenyegetés honnan érkezett. Az okostelefonok gyártói, az alkalmazások üzemeltetői egyaránt a dokumentumok hatálya alá vonhatók. Fontos azonban hangsúlyoznunk, hogy a magánélet, privátszféra védelméhez fűződő jog az Emberi Jogok Európai Egyezménye alapján nem korlátok nélküli. A hatóságok ugyanis megsérthetik ezen jogokat jogszerű indokokkal, mint amilyen a nemzetbiztonsági, közbiztonsági, közegészségügyi vagy közerkölcsbeli hivatkozások, valamint mások szabadságjogainak biztosítása esetében is jogosultak beavatkozni az egyén privátszférájába. Az EJEB az Uzun v Németország ügyben[30] kimondta, hogy a GPS segítségével történő megfigyelés és ezáltal az érintett lokalizációs adatainak hozzájárulás nélküli kezelése és felhasználása arányos beavatkozás volt az érintett magánéletébe az Egyezmény értelmében, ugyanis a nemzetbiztonsági szolgálatok a terrorizmus elleni küzdelem során a közbiztonság és a „demokratikus társadalom érdekében" szükségszerűen jártak el. E körben a hatósági kötelezések, melyek címzettjei a mobil alkalmazások üzemeltetői felülírhatják az egyén privátszférájának védelmét, amennyiben megfelelnek az Egyezmény 8. cikk (2) bekezdésében foglalt korlátozásoknak.

Az Európai Unió általános adatvédelmi rendeletét kiegészítő és azt a digitális világra specializáló e-Privacy irányelv, melyet a tervek szerint a készülő e-Privacy rendelet vált majd fel modernebb szabályokkal,

28 Brkan Maja – Psychogiopoulou Evangelia: Court, Privacy and Data Protection in the Digital Environment, Edward Elgar Publishing (2017) 132.

29 Brkan – Psychogiopoulou: i..m. 125.

30 Uzun v. Germany, 35623/05.

kifejezetten tartalmaz rendelkezéseket az okostelefonok használóinak védelmében. Az e-Privacy irányelv megkülönböztet forgalmi adatokat és lokalizációs adatokat. A lokalizációs, illetve az irányelv magyar fordításában helymeghatározó adat egy nyilvánosan elérhető elektronikus hírközlési szolgáltatás felhasználója végberendezésének földrajzi helyzetét jelző, az elektronikus hírközlő hálózatban kezelt minden adat[31], míg forgalmi adatnak egy közlésnek az elektronikus hírközlő hálózaton keresztül történő továbbítása vagy erre vonatkozó számlázás céljából kezelt minden adat minősül[32]. A GDPR 4. cikkének (7) bekezdése értelmében pedig valamennyi alkalmazásfejlesztő adatkezelőnek minősül, amennyiben az okostelefonon tárolt vagy megosztott személyes adatokat kezel, így lényegében a GDPR teljes kötelezettségkatalógusa alkalmazandó ezen alkalmazások, azaz a digitális kényelmi szolgáltatások üzemeltetőire is. A lokalizációs adatokat a mobilalkalmazások üzemeltetői ennek értelmében kezelhetik az eszközön futó operációs rendszer üzemeltetőjétől függetlenül is.[33] Ennek egyik megjelenése formája lehet, amikor az operációs rendszer üzemeltetője az, aki az általa gyűjtött adatokat továbbadja az alkalmazásban. Éppen ebből a megfontolásból az operációs rendszereket üzemeltető vállalkozások a saját szolgáltatásaik minőségének javítása céljából beszerzett lokalizációs adatok vonatkozásában, de a szintén általuk működtetett alkalmazásbolt (*app store*) vonatkozásában is adatkezelőknek minősülnek, hiszen a fogyasztó által letöltött alkalmazásokat rögzítik, valamint azok belépési információit, az azokban tárolt fizetési információkat tárolják. A GDPR 5. cikk (1) bekezdés (c) pontjában deklarált adattakarékosság megköti az alkalmazásfejlesztők és az operációs rendszert üzemeltetők kezét is abban a tekintetben, mire használhatják az általuk kezelt adatokat. Az operációs rendszer üzemeltetője értelemszerűen saját szolgáltatásának minőségét javítandó, míg az alkalmazásfejlesztő az alkalmazás által kínált funkciók működését biztosítandó jogosult csupán a lokalizációs adatok kezelésére. Az adattakarékosság azonban e körben több kérdést is felvet. A minőség

31 Elektronikus hírközlési adatvédelmi irányelv, 2. cikk c) pont.

32 Elektronikus hírközlési adatvédelmi irányelv, 2. cikk b) pont.

33 Bu-Pasha Shakila – Alen-Savikko Anette – Makinen Jenna – Guinness Robert – Korpisaari Paivi: EU Law Perspectives on Location Data Privacy in Smartphones and Informed Consent for Transparency, European Data Protection Law Review, 2016/2, 312.

javításának egyébként az érintett fogyasztó szempontjából is méltányolható célja nehezen objektivizálható, és nehezen állapítható meg sok esetben, hol húzódik a szükséges és az elégséges adatkezelés határvonala. Egy példával érzékeltetve egy étteremkereső és ajánló alkalmazás, melyben a fogyasztó letárolta számos személyes adatát (pl. név, születési idő, lakcím, telefonszám, kártyaszám, helymeghatározást segítő adat, ételallergiák, konyha preferenciák, tipikus partnerek stb.) értelemszerűen felhasználja ezeket az adatokat az éttermek keresése és ajánlása során, azonban át is adja ezen adatokat vagy azok egy meghatározott körét annak az étteremnek, ahová a keresést követően a fogyasztó asztalfoglalást indít. A GDPR ugyan kivételként rögzíti az adatvédelmi követelmények érvényre juttatásának főszabálya alól azt az esetet, amikor az adatkezelés az alkalmazás alapvető funkcionalitásának kiszolgálásához és biztosításához elengedhetetlen[34], azonban értelmezésre szorul mit is értünk alapvető funkciókon. Az előbbi példa mentén haladva vajon csupán a releváns találatok érdekében vagy már az asztalfoglalás és az annak nyomán megvalósuló étteremlátogatás előkészítése érdekében történő adatkezelés is alapvető funkció körébe értett? A kérdésre adandó válasz során tagadhatatlan, hogy a digitális kényelmi szolgáltatások meglehetősen szubjektív szűrőn keresztül megítélt funkcionalitásait vagyunk kénytelenek elemezni. E körben pedig arra a következtetésre kell jutnunk, hogy a kérdésben állásfoglaló jogalkalmazó saját szubjektív értékítélete nélkül aligha lehet minden oldalról védhető formában indokolni a választ. Éppen ez adja a GDPR-ban foglalt, az adatvédelem és a kényelmi szolgáltatás célkitűzéseinek megvalósulása közötti balansz biztosítására született szabály sérülékenységét, relatíve alacsony hatásfokát.

Ezzel elérkeztünk a másik, az európai adatvédelmi jogban és a tagállamok polgári jogi személyiségvédelmi szabályai között a talán legfontosabb garancia elemzéséhez, az érintett adatalany hozzájárulásán alapuló adatkezelés digitális kényelmi szolgáltatásokkal összefüggésben történő vizsgálatához. A GDPR szabályait értelmezve a hordozható eszközökön tárolt adatok, például a helymeghatározó adatok kezelése során az eszköz használója jogosult az operációs rendszer üzemeltetője kilétének megismerésére, az alkalmazás

34 Általános adatvédelmi rendelet, 6. cikk (1) bekezdés (f) pont.

üzemeltetőjének vagy fejlesztőjének megismerésére, akik mindannyian adatkezelőknek minősülnek. Az érintett adatalany jogosult továbbá arra, hogy az adatkezelés célját megismerje és az adatkezelés során a személyes adatot megismerő személyek köréről tájékoztatást kapjon. Joga van továbbá ahhoz is az adatalanynak, hogy hozzáférjen a kezelt adatok köréhez, valamint helyesbítést kérjen a kezelt adatokkal kapcsolatban.[35] A GDPR adatkezelési jogalapjai körében előkelő helyet foglal el az érintett hozzájárulásán alapuló adatkezelés lehetősége. Az ilyen, érintettől származó hozzájárulásnak azonban három követelménynek kell megfelelnie:

– az érintett szabad akaratából megadott hozzájárulás;
– az adott adatkezelési tevékenységhez történő speciális hozzájárulás;
– az azt megelőző tájékoztatás birtokában megadott hozzájárulás.

Az érzékeny személyes adatok kezelése során az adatkezelés általános tilalma alól szintén az érintett hozzájárulása adhat felmentést. A jelenleg hatályos e-Privacy irányelv szintén megköveteli, hogy a hálózatüzemeltetők a helymeghatározó adatok kezelését megelőzően szerezzék be az érintett hozzájárulását, melyet részletes, az adatkezelés célját érintő tájékoztatásnak kell megelőznie. Az irányelv világos és egyértelmű információk megadásának kötelezettségét írja elő a szolgáltatók oldalán.[36] Az irányelv 9. cikke a helymeghatározó adatok kezelésével kapcsolatos tájékoztatás tartalmát részletesen is listázza:

– az adatkezelés típusa;
– az adatkezelés célja;
– az adatkezelés időtartama;
– történik-e adattovábbítás harmadik személyek részére.

Az irányelv arra is lehetőséget biztosít az érintettek számára, hogy amennyiben a forgalmi adatok kezelésén túl a helymeghatározó adatok kezeléséhez is hozzájárultak, a hálózathoz való minden egyes csatlakozás alkalmával, illetve minden egyes közléstovábbítás esetén letilthassák az ilyen adatok kezelését (9. cikk (2) bekezdés). Ez a rendelkezés teszi azt lehetővé, hogy a fogyasztó

35 Bu-Pasha et al.: i. m. 315.
36 Elektronikus hírközlési adatvédelmi irányelv, 5. cikk (3) bekezdés.

a generális adatkezelési hozzájárulás helyett alkalmanként, használatonként dönthessen az adatkezeléshez történő hozzájárulásáról. Számos esetben azonban a fogyasztók ezt a számukra kínált jogosultságot kényelmetlen zavarásként értékelik, és az alkalmazás üzemeltetője, illetve fejlesztője is azt tapasztalhatja, hogy a hozzájárulás esetenkénti beszerzése az alkalmazás használatától fordítja el a fogyasztókat, jelentős hátrányt okozva neki a piaci versenyben. Bár az irányelv nem rendelkezik a letiltás lehetővé tételének formájáról, a gyakorlatban két megoldás alakult ki. Az egyik, kétségtelenül szövegkonformabb elképzelés szerint az alkalmazás minden megnyitása során újra és újra beszerzi a fogyasztó adatkezeléshez történő hozzájárulását. Ez a megoldás a már említett kényelmetlen zavarást sok fogyasztónál biztosan megvalósítja. A másik megoldás az alkalmazás, operációs rendszer szintjén – legtöbbször egy beállítások menüpont alatt – teszi lehetővé, hogy a fogyasztó az alkalmazás első futtatásakor megadott hozzájárulását visszavonhassa. Ez a megoldás ugyan kiiktatja a kellemetlen zavarást a hozzájárulási rezsimből, azonban olyan extra cselekvést és tudatos magatartást, nem egyszer magasabb szintű informatikai felhasználói képességeket is feltételez, amellyel a fogyasztók jelentős része nem rendelkezik, így külső segítség nélkül a hozzájárulás visszavonásának lehetősége számukra pusztán üres deklaráció marad. A GDPR meglehetősen ellentmondásosan fogalmazza meg az adatkezelési hozzájárulásokkal szembeni követelményeket. A rendelet az érintett akaratának önkéntes, konkrét és megfelelő tájékoztatáson alapuló, valamint egyértelműen kinyilvánított közléseként definiálja a hozzájárulást.[37] A GDPR hozzájárulással kapcsolatos feltételei között a következő kiegészítő elvárásokat is megtaláljuk:

– a személyes adatok különleges kategóriáival kapcsolatban – ahová a biometrikus azonosítók is sorolhatók – a rendelet külön hozzájárulás beszerzésének kötelezettségét írja elő, így e körben az adatkezeléshez általában adott felhatalmazás nem elegendő adatkezelési jogalap (9. cikk);

37 Általános adatvédelmi rendelet, 4. cikk 11. pont.

– az adatkezelőt terheli annak bizonyítása, hogy az érintett a hozzájárulását megfelelő tájékoztatás birtokában adta meg (7. cikk (1) bekezdés);
– több érintetti nyilatkozat beszerzése esetén az adatkezeléshez történő hozzájárulásnak más nyilatkozatoktól egyértelműen megkülönböztethetőnek, érthetőnek és könnyen hozzáférhetőnek kell lennie (7. cikk (2) bekezdés);
– a hozzájárulást ugyanolyan könnyen visszavonhatóvá kell tenni, mint amilyen könnyű módszerrel azt az érintett megadhatta (7. cikk (3) bekezdés).

A fenti kiegészítő követelmények ismeretében már kérdéses, hogy az operációs rendszer vagy az alkalmazás beállításainak szintjén visszavonható hozzájárulás megfelelő garanciákat ad-e az érintettnek. Véleményünk szerint nem, hiszen a fogyasztó olyan, az alkalmazás használatához megkívánt többletinformatikai ismereteire épít, amely már nem várható el az adatalanytól a saját adatainak védelmét biztosító reális intézkedések körében. Éppen ezért az a gyakorlat lehet kívánatos, a kényelmi szolgáltatásokkal is összeférő és a GDPR követelményeinek is megfelelő, ha az alkalmazás első futtatásakor kért hozzájárulás megadását követően egy rövid, a hozzájárulás beszerzésétől egyértelműen megkülönböztethető tájékoztatás is megjelenik, melyben a fogyasztó információkat kap a hozzájárulás visszavonásának lehetőségéről és a technikai megvalósítás lépéseiről.

A fenti, európai adatvédelmi jogban megjelenő követelményeket figyelembe véve és azokat a digitális kényelmi szolgáltatások piacára vetítve a következő gyakorlati megvalósítási modellt tartjuk szabályozáskonformnak és a fogyasztó információs önrendelkezési joga szempontjából fairnek:

– Már az adott szolgáltatást megjelenítő alkalmazás telepítése során információt kell nyújtani a fogyasztó számára, hogy az alkalmazás bizonyos funkcióinak használatához mely adatok milyen típusú kezelése szükséges. Ennek megvalósítására az alkalmazásbolt alkalmazásról adott leírásában kell egyértelműen, az alkalmazás funkcióinak bemutatásától jól elkülönített helyen megjelennie.

- Az alkalmazás első futtatásakor felugró üzenet formájában adjon tájékoztatást az adatkezelés céljáról, a kezelt adatok köréről, és az esetleges adattovábbításról, majd ehhez kérje a fogyasztó kifejezett hozzájárulását.
- Az adatkezeléshez adott hozzájárulást követően azonnal jelenjen meg egy üzenet, amely a fogyasztót tájékoztatja a hozzájárulás visszavonásának lehetőségéről, valamint arról, ezt a visszavonást milyen módon (technikai lépések segítségével) teheti meg.
- Az adatkezelési hozzájárulás kifejezett és külön hozzájárulás nélkül nem jogosíthatja fel az alkalmazásfejlesztőt és üzemeltetőt arra, hogy az alkalmazásnak futtatási hardverkörnyezetet adó eszközön található egyéb adatokhoz hozzáférjen és azokat gyűjtse.
- Olyan új alkalmazásba épített funkciókhoz történő hozzáférés esetén, melyek korábban nem kerültek elő a használat során, az adatkezeléshez specifikus hozzájárulásokat kell beszerezni, az első futtatáskor kért hozzájárulás és azt megelőző tájékoztatás körében már leírt módon és formában.
- Amennyiben az alkalmazás a fogyasztó kontaktlistájához való hozzáférést igényli, a fogyasztó számára lehetőséget kell biztosítani arra, hogy a kontaktokból fehér és fekete listát egyaránt felállíthasson, azaz kiválaszthassa azokat a kontaktokat, akikkel meg kíván osztani adatokat, illetve akiknek nem enged hozzáférést ezekhez az adatokhoz. A generális, valamennyi kontakt számára nyitva álló megosztás lehetősége nem elfogadható.
- Minden olyan esetben, amikor a szolgáltató adatkezelési szabályzata megváltozik, ennek tényéről, a változások lényegének bemutatásáról, valamint a szabályzat megismerésének lehetőségéről és módjáról tájékoztatni kell a fogyasztót, és adatkezelési hozzájárulásának megújítását be kell szerezni.

4. Az önszabályozás jelentősége és a transzparencia hiánya

A digitális szolgáltatások piacán a jogi szabályozás természetszerű korlátai már legalább egy évtizede jól ismertek. A gyorsan változó technológia generálta új szolgáltatásokra a jog nagyon lassan, gyakran a technológia alkalmazásának megszűnését vagy kivezetését követően reagál csupán. A jogi szabályozás évtizedeken keresztül technológia-semleges megoldásokat hirdető hozzáállása lassan változik meg az Európai Unió és a tagállamok adatvédelmi rezsimjének szintjén egyaránt. Éppen ezért egy olyan, a piaci verseny által indukált önszabályozás emelkedik ki az adatvédelmi biztosítékok rendszeréből, mely részben a felelősségi jogi előírások és azok értelmezése, részben a piaci versenyben elérhető pozíciók javításának célkitűzéseitől motiváltan a digitális szolgáltatásoknak terepet engedő eszközök gyártói, valamint a keretprogramok, operációs rendszerek üzemeltetői oldalán egyre nagyobb jelentőséggel bír. A polgári jogi felelősség körében a személyiségi jogok tiszteletben tartásának kötelezettsége az elmúlt évtizedben számos tagállami és nemzetközi bírósági döntésben is megjelenve olyan aktív cselekvési kötelezettséget ró a közvetítő szolgáltatókra, melyek alapján a *notice and take down* megközelítésen jelentősen túlmutató módon válnak a jogsértéseknek teret engedő közvetítő szolgáltatók gyakran a felelősség elsődleges alanyává.[38] A privátszféra titokban tartása és érintett általi kontrollja pedig egyre nagyobb számú fogyasztó számára válik fontos céllá a digitális térben kifejtett cselekvéseik során, így egy erősödő fogyasztói tudatosság is megfigyelhető a vásárlási döntések hátterében, kifejezetten adatvédelmi elvárások által motiválva.

Az önszabályozás egyik legismertebb megjelenési formája, amikor az alkalmazásfejlesztőkkel szemben szigorú adatvédelmi követelményeket, elvárásokat terjeszt az alkalmazásboltot üzemeltető vállalkozás. Mindaddig nem kerülhet fel az alkalmazás az áruházba, és ezáltal nem válhat elérhetővé a fogyasztók számára, amíg az áruházat üzemeltető vállalkozás nem győződik meg arról, hogy az alkalmazásfejlesztő betartotta az adatvédelmi követelményeket. Az Apple által üzemeltetett és valamennyi Apple által gyártott eszközön hozzáférhető App Store ezt a politikát követi. Az önszabályozás jelen esetben

38 Leenes et al.: i. m. 154.

komoly védelmet jelent a fogyasztók számára, hiszen az Apple platform népszerűsége és elterjedtsége a világban van annyira jelentős, hogy az alkalmazásfejlesztők ritkán negligálják az App Store-t. Az Apple az elmúlt három évben jelentős fejlesztéseket eszközölt a mobil eszközeihez kapcsolt operációs rendszer mint keretplatform adatvédelmi beállításait illetően is. A fogyasztók számára egyre szofisztikáltabb konfigurációs lehetőséget enged azon vonatkozásban, hogy rendszerszinten, illetve alkalmazásokra specializáltan dönthesse el a fogyasztó, milyen személyes adatát hogyan engedi kezelni. Erre kiváló példa a helymeghatározási adatok sorsáról való döntés iOS platform alatti kezelése. A fogyasztó dönthet arról, hogy egyáltalán nem engedélyezi a rendszer és annak alkalmazásai számára a helymeghatározási adatok kezelését, vagy beállíthatja, mely alkalmazások milyen esetben (pl. csak az alkalmazás használatakor vagy általánosságban) férhetnek hozzá ezekhez az adatokhoz.

A másik fontos önszabályozási kérdéskör sokkal inkább technológiához kötött. A biometrikus azonosítók – ahogyan arról már fentebb szó esett – egyre inkább központi technológiaként jelennek meg a digitális kényelmi szolgáltatások működése során, hiszen egy kényelmes, a fogyasztó oldalán minimális közreműködést igénylő, mégis biztonságos és alacsony hibarátával dolgozó jogosítási lehetőséget kínálnak. A biometrikus azonosítók tárolása azonban kétféle módon történhet. A fogyasztó számára kényelmesebb megoldás, amely lehetővé teszi, hogy egyszer beolvasott azonosítóit eszközök között is átvihesse, amennyiben ugyanazon profillal van bejelentkezve több eszközön. Ilyenkor a biometrikus azonosítót nem lokálisan, az adott eszközön, hanem az operációs rendszert üzemeltető vállalkozás által működtetett szervereken tárolják. Ez a lehetőség azonban további titkosítási és biztonsági intézkedéseket igényel, hiszen az operációs rendszert üzemeltető vállalkozás hozzáférhet ezekhez az azonosítókhoz. A vele szemben való védelem érdekében felmerülhet az a lehetőség, hogy az adatokat számos fájltöredékké szedik szét, ezeket külön felhőkben, más-más titkosítási algoritmusokkal ellátva tárolják, és alkalmazásukkor, emberi beavatkozást lehetetlenné tevő módon kapcsolódhatnak össze a fájldarabkák egységes fájllá.[39] Ez a megoldás

39 Sammons: i. m. 74.

azonban mindig magában hordozza annak a lehetőségét, hogy a rendszert működtető vállalkozás valahogy mégis hozzá tud jutni az adatokhoz. A másik megoldás, amely szintén egyelőre jogi kötelezettség nélküli technológiai döntés a vállalkozások oldalán, hogy a biometrikus azonosítók lokálisan, az adott eszköz valamely hardver komponensében kerülnek tárolásra. Az eszköz cseréje vagy másik eszköz használata esetén minden eszközön be kell olvasni az azonosítókat. Ez egy, az adatvédelem szempontjából, sokkal biztonságosabb azonosítási megoldás, hiszen maga a rendszert üzemeltető vállalkozás sem tud az eszköz nélkül az adatokhoz hozzáférni.

A fenti lehetőséget azonban kizárólag a vállalkozások saját választásától függnek, és bármiféle jogi kényszerítő erő nélküliek. Az Android platform például jóval kevesebb biztonságot kínál az adatvédelem terén, és a számos fogyasztó által nem ismert beállítások egyik rejtett bugyrában kapcsolható ki az az alapbeállítás, amely a helymeghatározási adatokat – bár anonim módon – gyűjti a felhasználóktól. Sajnos az internetre egyébként nem kapcsolódó eszközökről is lehetséges az adatgyűjtés, hiszen a számos hardverkomponens (pl. kamera, mikrofon, giroszkóp stb.), amit a fogyasztók netkapcsolat nélkül is használnak, szintén segíthet egy lokalizációs térkép összeállításában.

Az önszabályozó mechanizmusok sem lehetnek azonban tökéletesek. Ezen állításunk igazolása érdekében álljon itt néhány példa az elmúlt két évből, nagy techvállalatok közelében megvalósult és nyilvánosságra került jogsértésekről.

2018 elején az amerikai politikában is nagy port kavart az, hogy fény derült arra, hogy a brit Cambridge Analytica cég Facebook felhasználók millióinak szerezte meg jogellenesen különböző adatait és használta fel azokat politikai célokra. A Guardian nevű újság már 2015-ben arról cikkezett, hogy a Cambridge Analytica jogellenesen gyűjtött adatokat az amerikai Ted Cruz szenátor számára.[40] A Facebook nem kommentálta a tényfeltárásokat, azt, hogy az ő felhasználóinak hogyan fért hozzá a Cambridge Analytica a hozzájárulásuk nélkül az adataihoz. Az igazi botrány akkor robbant ki, amikor

40 Our Cambridge Analytica scoop shocked the world. But the whole truth remains elusive. [Elérhető: https://www.theguardian.com/uk-news/2018/dec/23/cambridge-analytica-facebook-scoop-carole-cadwalladr-shocked-world-truth-still-elusive (letöltés dátuma: 2019. január 04.).]

2018 márciusában a Cambridge Analytica egy korábbi alkalmazottja a neve felvállalásával kitálalt. A megszerzett adatokat arra használtak fel, hogy minden eddiginél személyre szabottabb módon keressenek fel és befolyásoljanak embereket a választások előtt, befolyásolva ezzel például az Amerikai Egyesült Államokban a választásokat. A cég egyébként, mielőtt kiderült, hogy jogellenesen, a felhasználók hozzájárulása nélkül gyűjtött információkat, büszkén hirdette magáról, hogy az ő kampányuknak köszönhető az, hogy Trump megnyerte az amerikai választásokat, vagy hogy a brexit mellett szavazott a brit lakosság többsége.[41]

2018 augusztusában nagy hírt kavart, hogy az Air Canada elismerte, hogy a mobiltelefonokon használt applikációját feltörték, és ezzel mintegy 20.000 utas adataihoz fértek hozzá.[42] Az Air Canada ráadásul nem az egyetlen légitársaság, akitől azutóbbi időszakban adatokat loptak. 2018-ban a Delta Airlines és a Virgin légitársaságok is elismerték, hogy a rendszerükből adatokat tulajdonítottak el ismeretlenek.[43] Az Air Canada esetében a légitársaság munkatársai augusztus 22-24. között észleltek szokatlan bejelentkezéseket az applikációjukba. A vizsgálatokat követően derült ki, hogy a felhasználók olyan személyes adatain kívül, mint a nevük, az email címük vagy a telefonszámuk, sokkal érzékenyebb személyes adatok is sérültek. Így az adatlopás áldozataivá váltak, az Air Canada mobilapplikációját használó utasok útlevélszáma, az útlevelet kiállító ország és annak lejárati dátuma, valamint az utasok születési dátuma, a nemzetisége és a tartózkodási országa. Az Air Canada légitársaság azt állította, hogy a bankkártyaadatok nem sérültek, mert azok titkosítva voltak tárolva.

A későbbi vizsgálatokból kiderült, hogy ezeket az adatokat az Air Canada légitársaság applikációja jogellenesen gyűjtötte és megküldte a légitársaságnak. Egy olyan adatlopásnak, amelyek a felsorolt adatokat érintik, kérdés, mi lehet a célja. Szakértők szerint nagy a valószínűsége annak, hogy a jogellenesen

41 Leaked: Cambridge Analytica's blueprint for Trump victory. [Elérhető: https://www.theguardian.com/uk-news/2018/mar/23/leaked-cambridge-analyticas-blueprint-for-trump-victory (letöltés dátuma: 2019. január 05.).]

42 Air Canada confirms mobile app breach. [Elérhető: https://techcrunch.com/2018/08/29/air-canada-confirms-mobile-app-data-breach/?guccounter=1 (letöltés dátuma: 2019. január 02.).]

43 Ibid.

gyűjtött adatokhoz hozzáférő illetéktelen személyek személyiséglopáshoz használják majd fel, melynek keretében ezen adatokat felhasználva bankokkal, telefonszolgáltatókkal vagy biztosítótársaságokkal kötnek majd szerződést online felületen – vagyis személyes megjelenési kötelezettség nélkül.[44] Mint azt az App Analyst elnevezésű szakértői oldal kifejtette a légitársaság applikációjáról, a jogellenes adatgyűjtést az okozta, hogy az egyes munkameneteken szereplő adatokat, melyekről képernyőfotókat készített a légitársaság, nem megfelelően takarta ki, így férhetett ahhoz hozzá akár a légitársaság valamely alkalmazottja, vagy más, a légitársaság szervereit meghackkelő személy.[45] A TechCrunch elnevezésű blog informatikusai a történteket vizsgálva 2019 elejére odáig jutottak a szálakat kibogozva, hogy nem csak az Air Canada rögzíti a felhasználóinak a tevékenységét, amit az applikációba belépve végeznek, hanem más nagy cégek, mint például hotelek, bankok, mobilszolgáltatók, más légitársaságok és utazással foglalkozó vállalkozások is hasonlóan járnak el. Tovább rontja a helyzetet, hogy a felhasználóknak nincs is tudomása arról, hogy minden appen belüli kattintásukról képernyőfotót készít és továbbít az applikáció alkalmazó vállalat, mivel nem kérik ehhez előzetesen a felhasználó engedélyét. A TechCrunch rájött arra, hogy közös a felhasználók előzetes engedélyét nem kérő és titokban adatot gyűjtő és azt nem biztonságos módon továbbító appekben, hogy mindegyik a Glassbox cég azon szolgáltatásait alkalmazza, amely arra hivatott, hogy a felhasználók az applikáció használata során formálódó élményét elemezzék. A Glassbox partnereit vizsgálva arra jutottak a szakértők, hogy nem minden app továbbítja a felhasználók különféle adatait, azonban kivétel nélkül mindegyikre igaz volt, hogy a felhasználó engedélye nélkül gyűjt adatot a felhasználótól.[46] Az Apple a TechCrunch informatikusainak megállapításaira reagálva, 2019. február 8-án (egy nappal a tényfeltárás eredményeinek közlését követően) egy szoftverfrissítést bocsátott az Apple termékeket használók rendelkezésére, melyben biztonsági problémákat orvosolt.

44 Air Canada app data breach involves passport numbers. [Elérhető: https://www.bbc.com/news/technology-45349056 (letöltés dátuma: 2019. január 02.).]

45 App Analysis: Air Canada. [Elérhető: http://theappanalyst.com/aircanada.html (letöltés dátuma: 2019. január 03.)]

46 Many popular iPhone apps secretly record your screen without asking. [Elérhető: https://techcrunch.com/2019/02/06/iphone-session-replay-screenshots/ (letöltés dátuma: 2019. február 07.).]

A TechCrunchnak 2019 év elején más, nagy botrányt kavaró felfedezése is volt. A XXI. században az emberek, különösen a fiatalok közötti egyik jelentős kommunikációs csatorna a Facebook, amely az utóbbi időben többször került a figyelem középpontjába adatkezelési botrányai miatt. A legújabb botrány azonban különös veszélyt jelent a felhasználókra, főként a fiatalabb generációra nézve. A Facebook az újabb fejlesztések kidolgozásához szeretett volna ötleteket szerezni a fiatalabb felhasználóktól. Ezért 2016-ban kampányt indított, melyben bevonja a 13 és 35 év közötti korosztályt, még fizetést is kínálva számukra közreműködésükért. A munkabér azonban jelképes, ugyanis a Facebook havi 20 dollárt fizet azért az azt vállaló felhasználóknak, hogy olyan információkhoz juthasson róluk, amivel eléri ezen célkitűzését.[47] A bevonzott fiatalokkal megkötött szerződés azonban nem tartalmaz néhány lényeges feltételt, például azt, hogy a Facebook a felhasználó Facebook profilján kívül minden olyan adathoz hozzáférhet, ami az adott egyén telefonján vagy mobileszközén létezik, így a privát elektronikus levelezéséhez; a küldött és fogadott fotókhoz és videókhoz; az interneten végzett valamennyi tevékenységhez. Vagyis egy olyan kémprogram tudatukon kívüli telepítéséről van szó, amely az egész életüket megfigyeli, rögzíti és továbbítja a Facebooknak.[48] Sokszor azt is nehéz felismerni, hogy a Facebookkal áll szerződéses jogviszonyban a felhasználó, mert más oldalakon keresztül adminisztrálják a szerződéskötési folyamatot, és más név alatt.[49] A „program" mind iOS, mind Android platformokon elérhető. A kémprogramról megjelent hírek után azonban az Apple elítélte a Facebook adatszerzési módszereit, és letiltotta az alkalmazást valamennyi iOS platformú eszközről.[50]

47 Facebook pays teens to install VPN that spies on them. [Elérhető: https://techcrunch.com/2019/01/29/facebook-project-atlas/?fbclid=IwAR345_Mz7HwN8_jyixNu-Z_jgXCqJIx5xhwVVmaAAsU6gXbMfBJcOeqFnXM&guccounter=1 (letöltés dátuma: 2019. január 30.).]

48 Ibid.

49 A projektben részt vettek például a BetaBound, az Applause és a uTest nevű oldalak.

50 Apple bans Facebook's Research app that paid users for data. [Elérhető: https://techcrunch.com/2019/01/30/apple-bans-facebook-vpn/ (letöltés dátuma: 2019. február 01.).]

A jövő útja

A digitális kényelmi szolgáltatások létjogosultsága nem megkérdőjelezhető napjaink digitális piacán. Az intenzív piaci verseny és az ebből kinövő innovációs kedv és a fogyasztók egyre növekvő elvárásai kényszerűen egyre komplexebb adatvédelmi kockázatokat is a felszínre hoznak. A digitális tér adatvédelmi kihívásaira egy technológia-semleges szabályozás soha nem lesz kellően hatékony válasz. A prevenció ugyanis ebben a körben a jogsértések körében uralkodó nagyfokú látencia és a jogsértések következményeinek enyhítése körében uralkodó viszonylagos hatástalanság miatt kiemelt jelentőséggel kellene, hogy bírjon. Alapelvi szintű elvárások, mint amilyeneket a GDPR az európai rezsimben megteremtett, egy megtörtént jogsértés orvoslása során biztosan segíthetik a jogalkalmazókat az incidens jogellenessé minősítésében, azonban a megelőzést hatékonyan nem szolgálják. Konkrét, a prevenciót elsődleges célként kitűző megoldások azonban a klasszikus jogszabályok szintjén biztosan nem képzelhetők el, hiszen a jogalkotási folyamatok e körben szinte kizárólagosan utólagos reakciót megtestesítő sajátosságai miatt mindig csak kullogni fog a piaci innovációk mögött. A legnagyobb techcégek azok, amelyek az önszabályozás erősítésével és saját piaci szemléletük adatvédelmet priorizáló elemekkel történő bővítésével képesek egy hatékony rendszert kialakítani.