Adatgyűjtési módszerek jogi szabályozása és a velük kapcsolatos biztonságtudatosság

Bernáth Áron, Fehér-Polgár Pál

Óbudai Egyetem, Keleti Károly Gazdasági Kar,

aron01010@gmail.com, feherpolgar.pal@kgk.uni-obuda.hu

Absztrakt: Az adatvédelem fontosságára először igazán 2019-ben figyelt fel a média és az átlagos internetező. Ekkor történt ugyanis, hogy nyilvánosságra kerültek az egykori Facebook (ma META) social media platform adatkezelési megoldásai. Ezelőtt is tudott volt, hogy a cég nem csak az oldalra feltöltött posztjainkat képeinket, az általa üzemeltetett üzenetküldő megoldásokat üzeneteinket képes megfigyelni, de akkor is követi a az aktivitásainkat, amikor éppen nem tartózkodunk az oldalukon. Tudott volt továbbá azt is, hogy ezeket az adatokat harmadik felekkel is megosztja.A figyelem azért irányult mégis rá, mert az adatkezeléssel megbízott egyik partnercégüktől több millió felhasználó adatait lopták el. Nem ez volt az első eset, hogy hackerek adatokat loptak. Például 2013 és 2016 között a yahoo összes felhasználójának adatához hozzáfértek támadók. 2017-ben az amerikai választási rendszer 198 millió szavazójának adtait lopták el. Mégis miért pont a Cambridge Analytica kapcsán nyitották fel szemüket a felhasználók, és követeltek nagyobb privát szférát maguknak?A kulcs talán abban rejlik, hogy a facebookon mind teljes személyünkben vagyunk jelen. A személyes adataink, amivel viszonylag sok adattárház rendelkezik (gondoljunk az államháztartásra és a nekik szoftvereket építő cégekre), viszont a facebook pillanatról pillanatra követi minden lépésünket bárhova kattintunk az interneten. Az így begyűjtött adatokból és a modern algoritmusokból olyan termékeket és szolgáltatásokat ajánl számunkra, amikre éppen csak gondolunk. (Jobban ismer minket, mint mi magunkat ahogy, azt a modern közmondás tartja). Ezekből az adatokból pedig újra felépíthetőek vagyunk.

Kulcsszavak: Adatgyűjtés, biztonságtudatosság

Adatvédelem

Az Adatvédelem (Data Privacy), mint emberi jog

Az ENSZ legfőbb emberi jogi irodája már évekkel ezelőtt arra a következtetésre jutott, hogy a magánélet tiszteletben tartása érdekében az adatvédelmet, mint emberi jogot szabályozni kell. [1]

Mivel azonban az emberjogi egyezmények, csak kormányokra vonatkoznak, akik megtagadhatják ezek végrehajtását és betartatását a magánvállalatok inkább normákat követtek. A GDPR, ami már az

bevezetőben is említett Cambridge Analytica 2018-as szivárgás alatt készülőben volt, megváltoztatta ezt az álláspontot és a vállalatokra is érvényes szabályozásokat hozott.

A vállalatoknak azt kell megérteniük, hogy pusztán azért, mert egy felhasználó megosztott egy információt egy platformmal vagy azon keresztül másokkal, még nem jelenti azt, hogy elvesztette az összefüggő adatok iránti magánéleti jogát. Az Európai Emberi Jogok Bírósága álláspontja szerint a rólunk szóló adatok még akkor is kiválthatnak magánéleti aggályokat, ha nem a személyünkhöz kötődő titkot jelentenek.[2]

Az Európai Unió jogrendszere még szigorúbban szabályozza az olyan személyes információkat. Ez azért fontos, mert amikor egy vállalat olyan adatokat gyűjt, elemez vagy oszt meg, amelyek az egyén személyes vagy érzékeny jellemzői, például a faji hovatartozása, vallási és/vagy politikai nézetei ami diszkriminációhoz vezethet - ahogy azt az állítólagosan elfogult lakáshirdetésekkel kapcsolatos folyamatos viták is mutatják a Facebookon.

Az olyan vállalatok, mint a Facebook, hatalmas, személyes adatokra épülő adattárházakat hoznak létre, ami ideális célpont lehet támadószándéknak.

Ezért az emberi jogi alapelvek betartása létfontosságú ezeknek a vállalatoknak, még akkor is, ha a felhasználók tudatosan megosztottak információkat magukról. Az emberi jogi bíróságok azt is elismerték, hogy a személyes adatok kezelésének majdnem minden lépése - a kezdeti gyűjtéstől az felhasználásig, a megőrzésig és az megosztásig - beavatkozhat a magánéletbe.

GDPR

Az GDPR (General Data Protection Regulation)[3] az Európai Unió által 2018-ban elfogadott jogszabály, amely az adatvédelemre és a személyes adatok védelmére vonatkozik az Európai Gazdasági Térségen belül. A GDPR számos rendelkezést tartalmaz, amelyeknek a célja az egyének személyes adatainak védelme, és az adatkezelők (például vállalatok, szervezetek) felelősségének szigorúbbá tétele. Nem csoda tehát, hogy ennek a létrejöttét a szilícium-völgyi vállalatok nem fogadták túl “sportszerűen”. 2020 decemberében kiszivárogtatott dokumentumok sokkoló hatást váltottak ki az EU szabályozó hatóságai között, amikor kiderült, hogy a technológiai óriások jelentős összegeket költöttek a már meglévő keretek elleni lobbizásra és aláaknázásra.[4] Évek óta a technológiai óriások lobbiznak a szövetségi adatvédelmi szabályozások ellen. Az óriáscégek keményen küzdöttek az Egyesült Államok első állami szintű fogyasztói adatvédelmi törvénye, a Kaliforniai Fogyasztóvédelmi Törvény (CCPA) ellen.

Azonban miután Kalifornia bevezette a saját törvényét,[5] ami sok más állam számára is példát mutatott, a technológiai vállalatok gyorsan megváltoztatták álláspontjukat. Azok most az "enyhébb" állami

adatvédelmi törvények támogatására lobbiznak, hosszú távú céljuk pedig egy üzletbarát, kevésbé szigorú szövetségi adatvédelmi törvény elfogadása.

Súlyos kritikával találta szembe magát Írország Adatvédelmi Bizottsága (DPC), amely az európai vezető szabályozó az adatvédelem terén. A technológiai óriáscégek, mint a Google, a Facebook és az Apple, mind európai székhellyel rendelkeznek Írországban, ami a DPC-t a nagy technológiai vállalatokkal vívott európai adatvédelmi harc középpontjába helyezi. A DPC-t súlyos kritikával is illette a magánélet védelmező Max Schrems, aki kritizálta a GDPR végrehajtásában mutatott hatékonyság hiányát. Schrems, akinek a Facebook ellen indított hosszú tárgyalása egy mérföldkő, a Schrems II. ítélettel zárult, ami az EU-USA adatforgalmat helyezte új, biztonságosabb alapokra.[6]

A GDPR hat alapra épül:

• Hozzájárulás: A személyes adatok kezelése általában tilos, hacsak azt a jog törvényesen lehetővé teszi, vagy az érintett személy hozzájárult az adatkezeléshez. Ez nagy lépésnek tűnik a GDPR előtti időkhöz képest amikoris az oldalaknak nem kellett beleegyezést kérniük a felhasználók monitorozásához. A GDPR értelmében az oldalra látogatás előtt az oldalnak minden a GDPR-ban deklarált funkciójához külön-külön a felhasználó beleegyezését kell kérnie.

• Szerződés: A felhasználónak és az adatok kezelőjének szerződést kell kötniük az adatok felhasználásának módjairól és feltételeiről. Illetve, hogy ezt a GDPR-ban meghatározott irányelvek és szabályok szerint történik. Ami előrehaladás a GDPR előtti időkhöz képest, hogy ha az adatok kezelője, az adatokat megosztaná egy harmadik féllel is, szabálysértést követ el, mivel a kötött szerződés csak a szerződő felekre vonatkozik, ha egy harmadik fél bevonása is történik a felhasználónak a harmadik féllel is szerződnie kell.

• Jogalap: A jogi kötelezettség jogalapjának használatához a kezelőnek fel kell mérnie, hogy a kezelés valójában "szükséges" a kötelezettség teljesítéséhez. Ha a személyes adatok kezelése nélkül is észszerűen teljesíthető a kötelezettség, akkor ez a jogalap nem lesz megfelelő. Vagyis a kezelők nem gyűjthetnek adatot például, ha a kattintásainkat szeretnék követni, de nem nyújtanak testreszabott tartalmat.

• Életbevágó jogalap: Személyes adatok kezelése az egyén életének védelme érdekében egy kevésbé gyakran alkalmazott jogalap, de ugyanakkor fontos figyelembe venni bizonyos konkrét helyzetekben, ahol más jogalapok nem megfelelőek. Ahogyan más jogalapok esetében, a kezelőknek meg kell fontolniuk, hogy a kezelés valóban szükséges-e az élet védelméhez. A kezelők valószínűleg erre a jogalapra támaszkodnak, amikor a személyes adatok kezelése szükséges valakinek az életének védelméhez, vagy súlyos fenyegetést jelentő esetnél, például egy gyermek vagy eltűnt személy esetében.

Például: A mentők egy lakóotthonba érkeznek, hogy segítsenek egy kritikus állapotban lévő lakó lakójának, aki eszméletlen, amikor a mentők megérkeznek. A lakó orvosi előzményeit és egyéb releváns egészségügyi adatait megoszthatják a mentőkkel, mivel ez szükséges az életfontosságú érdekeik védelméhez - még akkor is, ha például a lakó korábban nem járult hozzá az ilyen célú adatmegosztáshoz.

• Közfeladat: Az Általános Adatvédelmi Rendelet (GDPR) egyértelműen megállapítja az 1. cikk végén, hogy a közintézmények nem támaszkodhatnak a "jogos érdekek" jogalapra annak igazolására, hogy a személyes adatok kezelése a feladatok végrehajtása során történik. Korábban ennek a fajta kezelésnek egy része jogos érdekeken alapult, de most a közintézményeknek meg kell fontolniuk, hogy a megfelelő jogalap a közérdekű feladatok végrehajtása vagy hivatali jogkör gyakorlása-e.

• Jogos érdekek: A "jogos érdekek" egy sokoldalú és rugalmas jogalap a személyes adatok kezeléséhez, amely olyan körülmények között alkalmazható, ahol a kezelési műveletek nem illeszkednek tökéletesen más jogalapok közé; azonban magával hordozza a kontrollerekre nehezedő kötelezettségeket is, hogy az általuk követni kívánt jogos érdekeket egyensúlyban tartsák az érintett személy jogaival és érdekeivel. Azok a kontrollerek, akik értékelik, hogy jogos érdekekre hivatkozva feldolgozzák az adatokat, a következő három elemet kell vegyék figyelembe ezen jogalap tekintetében:

a) azonosítani egy jogos érdeket, amelyet ők vagy egy harmadik fél követ;

b) kimutatni, hogy az érintett személy személyes adatainak tervezett kezelése szükséges a jogos érdek eléréséhez;

c) egyensúlyozni a jogos érdeket az érintett személy érdekeivel, jogaival és szabadságaival.

Ezek csak a legfőbb alapok, rengeteg más konkrét szabályozás létezik még, melyek a későbbiekben említésre kerülnek.

Facebook adatvédelmi szerződése

Ebben a fejezetben azt fogjuk vizsgálni, hogy pontosan milyen adatokat tárol rólunk a facebook és hogy ez hogyan áll összhangban a GDPR alapelveivel és szabályozásaival. Ezeket magunk is megtekinthetjük a Meta Privacy Policy szekciójában. Ezek nem csak a facebookra hanem a Meta összes platformjára vonatkoznak, mint Instagram, Whatsapp.

Ezek többek között:

• Amit az oldalra kirakunk, mint posztok, kommentek.

• Amit a facebook kamera alkalmazásnak átadunk. Ezt akkor tesszük amikor maszkokat, filtereket rakunk a képeinkre még akkor is, ha a képet csak saját telefonunkon tároljuk.

• Üzenetek, amiket ezeken a platformokon váltunk. Ezek az titkosítás miatt a Meta dolgozói számára nem láthatóak, csak az üzenet jelentése esetén fejtik vissza.

• Metadata: információ az adatról magáról: hol és mikor készült a kép. Vagy az üzenet típusa. Ennél a résznél hozzáteszik, hogy ezeknek az elemeknek a gyűjtése a hatályos törvények szerint történik. Viszont a hatályos törvények mező nem jelenít meg linket, ami a hatályos törvényekhez vezetne minket, vagy bármilyen olyan magyarázatot nyújtana, hogy pontosan mi alapján járnak el. Ez már egy lehetséges GDPR kihágás.

• Tartalom: ahogy és amennyit érintkezünk vele: pl.: hogy reagálunk egyes reklámokra.

• Használt applikációk pl.: játékok

• Vásárlások és tranzakciók az oldalon (Meta Pay), bankkártya adatok címek.

• Interakció különböző facebook-os oldalakkal

Ezen felül azt látjuk még ezen az oldalon, hogy opcionális megosztható a bőrszínünk, vallásunk, szexuális orientációnk, politikai nézeteink, egészségügyi állapotunk, nézeteink, vagy bármi hasonló privát információ.

Itt sem kapunk túl sok információt, mindössze annyit, hogy ezekre országonként különböző titoktartási törvények vonatkoznak. Ilyen törvények leginkább csak Európában vannak, az Egyesült Államokban például a facebook előszeretettel zúdít összeesküvés elméleteket kisebbségekre, vagy Qanon propagandát republikánus szavazókra. Nyilván mondhatjuk azt, hogy akkor nem töltünk fel profilképet, hogy a Meta még véletlenül se tudja, hogy milyen rasszhoz tartozunk, vagy nem adunk meg születési dátumot. Azonban, ezeket az információlat saját szándékunk nélkül is kiszolgáltatjuk a facebooknak, ugyanis, ha valaki más tölt fel egy képet, amin minket is bejelöl, vagy említést tesz ezen információkról valakinek üzenetben, az adatokat akkor is megosztottuk, viszont az önkéntesség hiányzik.

Ezen kívül gyűjtve van még hálózatunk, ip címünk, ezen kívül mindent, amit a készülékünkön csinálunk, akkor is, ha a facebook nincs megnyitva, ugyanis a facebook tracker-t helyez a készülékeinkre, amik az felhasználók számára láthatatlanok. Ezáltal az eszközünk olyan adatot küldhet, mint pl.: GPS lokáció, kamera és fotók, illetve az ehhez köthető metadata. Legutoljára a 2018-as szivárogtatás körüli botrányban lett nyilvánosságra hozva adat arról, kivel osztja meg az akkor még Facebook a gyűjtött adatokat, A felsorolásban szinte minden nagyobb szilícium-völgyi vállalat megtalálható volt, mint az Amazon, Spotify

vagy Netflix. Ez volt a legutolsó alkalom, hogy a partnercégek nevei nyilvánosságra kerültek, azóta a Meta nem ismerteti, hogy pontosan kivel és milyen kapcsolatban áll, kivel oszt meg információkat, vagy kitől kap. Azt viszont tudjuk milyen információkat szerez be a platform a partnereitől.

• Tranzakciós adatok, a partnerek saját oldalán vagy a partner által használt tracker segítségével begyűjtött adatok: bankkártyaszám, címek, fizetés módja, összeg és a megvásárolt termékek.

• A partnerek által üzemeltetett szolgáltatások, és azok használatának módja, ideje, időtartama akár online vagy személyesen.

• A partnerek megosztják az email címünket, cookie információnkat (azon információk amiket a partner cookie-k összegyűjtöttek rólunk), és ezek alapján össze tudnak kapcsolni minket a fiókunkkal.

• Továbbá a partnerek megosztják a Meta-val a velünk való kommunikációjukat, hogy ez mit takar azt a Meta privacy policy-je szerint a partner privacy policy-ben kellene elolvasnunk, viszont ahogy említettem a partnerek nem nyilvánosak így nem tudhatjuk pontosan mit kellene olvasnunk.

Adatgyűjtési módszerek és eszközök

Mi az a Cookie?

Mindenki hallott már internetes cookie-ról de, miert kérdezi meg minden weboldal, hogy elfogadjuk- e őket?

Valójában ezek nem arra valók, hogy egy kávé vagy tea mellé elnassoljuk őket, hanem a modern internetezés elengedhetetlen eszközei.

A sütik segítik a webfejlesztőket abban, hogy személyre szabott és kényelmes webes élményt nyújtsanak nekünk. Egyszerűen fogalmazva, a sütik lehetővé teszik a weboldalaknak, hogy emlékezzenek ránk, a bejelentkezéseinkre, a bevásárlókosarainkra és még sok egyébre. De ugyanakkor magukban hordozhatnak személyes információk gazdag forrását is, és súlyos veszélyt jelenthetnek a magánszféránkra. [7]

A sütik kis szöveges fájlok, amelyek egyedi adatokat tartalmaznak a számítógépünk azonosításához a hálózaton. Amikor meglátogatunk egy weboldalt, a böngészőnk kap egy sütit, vagyis egy rakás karaktert egy sütifájlban tárolva, amit a gépünk a böngésző mappájában helyez el a merevlemezen. Amikor a következő alkalommal ugyanazt a weboldalt látogatjuk meg, a böngésző visszaadja a sütiket az azonosításunkhoz.[8][9]

A sütik valóban tartalmaznak adatot, ami általában magában foglal egy egyedi azonosítót és egy weboldal nevét. Egy süti tartalmazhat olyan személyazonosító információkat is, mint a nevünk, címünk, e-mail címünk vagy telefonszámunk, ha ezt az információt a weboldalon megadtuk.

Egy egyszerű példa a sütikre az, amikor egy weboldalt megnyitunk, és a felhasználónevünk és jelszavunk automatikusan kitöltődik. A sütik biztosították a bejelentkezési információinkat a weboldal számára.

Egy másik példa az, amikor az Amazonon online vásárolunk, és olyan tételeket találunk a kosarunkban, amik még mindig benne vannak az előző vásárlási rohamunkból. Ebből is látjuk, hogy a sütik sokfélék lehetnek a következőkben megkísérlem bemutatni valamennyi fajtáját.

Mi az a Tracker?

A tracker egy olyan mechanizmus, amely képes követni a felhasználó minden lépését legyen az kattintás, lokáció, privát fájlok és hasonlók. A tracker önmagában nem egy technológia, hanem olyan technológiák, amelyek végső célja a fenti cselekmények megvalósulása és ennek elérése érdekében technológiák széles tárházát használja fel ellenünk. A kezdetekben csak a sütik által nyújtott technológiát használták, azonban már sokkal szofisztikáltabb és hatékonyabb módjai is vannak az adatgyűjtésnek.

• Tárolóalapú mechanizmusok: A következő nyomkövetési mechanizmusok csoportja az adatok explicit tárolásán alapul a felhasználók számítógépén. Ezek a módszerek úgy tűnik, hogy a leggyakrabban használtak. Képesek felismerni a böngészőt, az operációs rendszert és a hardware-t. Ezek közül mindegyik mechanizmus a felhasználók személyes adatainak a legnagyobb veszélyét jelentette közvetlenül az elkészítése után. Idővel a böngészők elkezdtek lehetőséget biztosítani ezeknek a tárolóknak a felhasználói kérelemre történő törlésére.

• Webes cookie-k: A web tracking legősibb formája a már bemutatott cookie-k. Méretük nem haladja meg a 4kb-ot, így a fejlesztők gyakran feldaraboltak nagyobb mechanizmusokat, ami viszont a hatékonyság csökkenéshez vezetett. Ezeket vagy egy Javascript API hívással vagy a HTTP request-be ágyazott Set-Cookie header-el küldik a felhasználó számítógépére. A Javascript-es Api-call-al egyszerűen megkerülhető a böngészők “ne engedélyezze a sütiket a harmadik féltől” beállítása, úgy, hogy a Javascript a kért oldal megjelenítése előtt egy harmadik oldalra navigál, ami igy közvetlenül helyezhet el tracker-eket a böngészőben, majd gyorsan visszanavigál az eredetileg kért oldalra. Előfordul továbbá, hogy egy weboldal által elhelyezett sütit megoszt más weboldalakkal is, amiket eddig nem látogattunk. Ezt általában olyan alkalmazások használják, mint a google, hogy fiókunkkal váltogathassunk az alkalmazások között, és ne kelljen újra bejelentkeznünk minden alkalmazásba.

• HTML5: A HTML új verziójában jelentősen növelhető a böngészőben tárolható adatok mérete. 4kb helyett 5mb-os fájlokat is el lehet tárolni, ami azt jelenti nem kell darabolni őket. Ezeket a Local vagy Session tárolóban tárolja a böngésző, tehát viszonylag könnyű megszabadulni tőlük.

• Cache-alapú mechanizmusok: A böngésző, saját teljesítménye javítása érdekében az általunk felkeresett weboldalakat, azok fájljait, képeit elhelyezi egy véges gyorsítótárban, hogy azok újra betöltése gyorsabb legyen, mint újra letölteni azt. A gyorsítótár a böngészőn belül, tehát helyileg fut, ha beírunk egy linket a címsorba, a böngésző először végigfut a gyorsítótárán hátha, nem kell újra felkeresnie a kívánt címet. A cache-alapú mechanizmusok a böngészőknek pont ezt a funkcióját támadják. A lényeg, hogy egy azonosítót tudjanak elhelyezni a web cache-ben, amit az oldal újra felkresésekor be tudjanak olvasni. Ezek a mechanizmusok kikerülnek olyan védelmi intézkedéseket, mint a proxy vagy a vpn.

• ET-tagek ás Last-Modified HTTP header-ek: Ezek az elemek mind a HTTP header részei. Az ET tag 81864-bit hosszú, így önmagában elég, hogy azonosítót helyezzenek el benne. A Last-Modified szintén nem csak előre meghatározott értékeket vehet fel. Amikor az oldal újra -látogatása megtörténik a HTTP request-ben el lesznek küldve a tárolt azonosítók.

• Működési gyorsítótár- alapú mechanizmusok: Működési gyorsítótárak olyan komponensek, amelyeket arra használnak, hogy információkat tároljanak a webböngészők által végzett műveletekkel kapcsolatosan, nem pedig a letöltött elemek másolatainak tárolására. Az ilyen tárolt információk tartalmazzák például az állandó átirányításokat, az azonosítási hitelesítési adatokat, vagy azoknak a tartományoknak a listáját, amelyeket együtt kell használni az HTTP Strict Transport Security (HSTS) használatakor.

• Fingerprinting: A mai talán legelterjedtebb módszer a fingerprinting. Ez egy JavaScript alapú módszer. Amint meglátogatunk egy oldalt a JavaScript szkriptek letöltődnek a számítógépünkre, ezeknek az instrukcióknak read jogosultsága van a számítógépünkön és ezzel a rendszerünk minden elmét láthatják. Ezután egy egyedi azonosítót adnak számítógépünknek, ez lesz a gépünk ujjlenyomata. Ez arra szolgál, hogy a követésünk egyszerűbbé váljon a weboldalak között. Mivel ezek az ujjlenyomatok nem függenek a tárhelyünktől nem lehet őket csak úgy kitörölni. A Javascript-nek viszont megvannak a határai, mivel minden böngészőn belül egyszerűen letiltható, ezért a fejlesztők már Java-t is használnak, mivel ezzel is egyszerű TCP kapcsolatokat létrehozni és nem letiltható a böngészőben.

• Hálózat és lokáció fingerprinting: Az érkező HTTP kérések fejlécének alapján egyik legkönnyebben meghatározható jellemző a felhasználó globális hálózati címe és IP- alapú földrajzi tartózkodási helye. Hálózati eszközök használatával a szolgáltatás képes azonosítani a tartomány nevét és a felhasználó internet szolgáltatóját. Ezzel a proxy szerverek is kimutathatóak A böngészőben beállított proxykat Flash

alkalmazások segítségével is lehet kikerülni, hogy felfedezzék a kliens valódi IP címét, amit például az Iovation és a ThreatMetrix is használ, amelyek a legnépszerűbb ujjlenyomat-szoftver fejlesztő vállalatok közé tartoznak. Több fontos jellemzőt is vissza lehet kapni Javascript függvényekkel, például a belső IP címet és a GPS koordinátákat. A kapcsolat teljesítménye (például letöltési és feltöltési sebességek, bejárási idő és jitter) kiszámítható JavaScript vagy Flash segítségével. Végül Java applet-ek használhatók a tűzfal jelenlétének észlelésére.

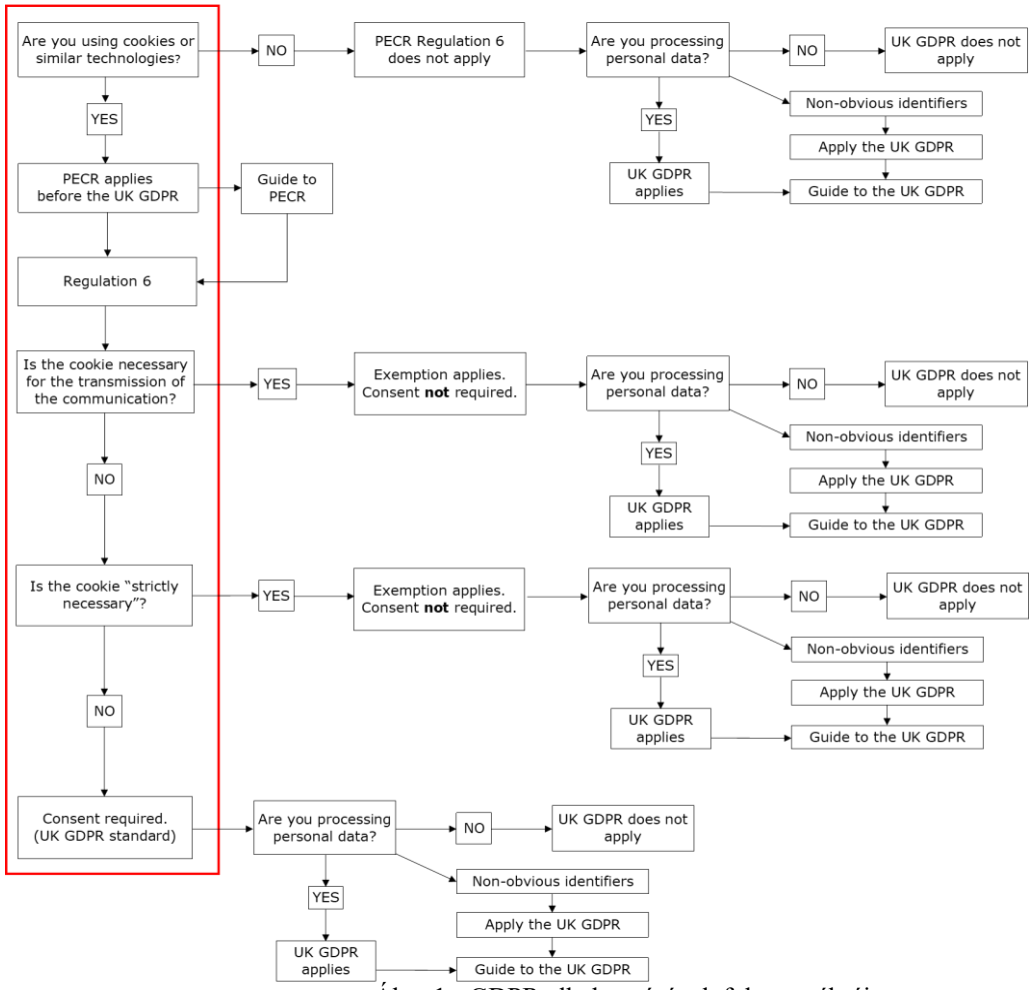
• Device fingerprinting: Ahogy azt a neve is mutatja ebben az esteben a hálózat helyett a tracker-t magán az eszközön helyezik el. Ez a fajta tracking képes információt gyűjteni a felhasználó egeréről, billentyűzetéről, gyorsulásmérőjéről, mikrofonjáról és kamerájáról. Továbbá az eszköz tracking mechanizmusok többsége teljesen független az operációs rendszertől vagy az eszköz típusától, ezért ez az egyik legnagyobb veszélyforrás a felhasználók privát szférájára nézve. Ez a fajta mechanizmus szélesen használt a weben mivel az elsődleges célja a csalók, hackerek kiszűrése különböző oldalakról vagy alkalmazásokról. Rengeteg cég fő profilja az ujjlenyomatozás. Ők könnyen implementálható plugin-eket gyártanak, mint például a fingerprintJS.

Jogi kérdések a tracking technológiák kapcsán

A GDPR szerint az ujjlenyomatozás egy kalap alá esik a sütikkel, vagyis nincs külön szabályozva. [10] Megismerve azonban a két technológiát, beláthatjuk, hogy a két mechanizmus eltér egymástól mind céljában, mind kivitelezésében. Az alábbi ábra bemutatja, pontosan mikor kell az adatok kezelőjének engedélyt kérnie, és mikor vonatkozik rá a GDPR. Bár az Egyesült Királyságban érvényes u.n. UK GDPR nem egyezik meg teljes mértékben az Európai Unió GDPR szabályozásával, de eltérésük a vizsgálatunk szempontjából indiferens.

Ahogy a mellékelt ábra is mutatja, nem szükséges beleegyezést kérni, ha az oldal működéséhez elengedhetetlen a süti, és az nem kezel személyes adatot. Emlékezzünk vissza, milyen paraméterek alapján ujjlenyomatoztuk a felhasználókat a gyakorlati példánkban. Olyan változókat használtunk, mint a böngésző verziója, font típusa, flash verzója, vagy még a legvadabb példákban is a kamera vagy billentyűzet típusa. A GDPR alapján nem személyes adatok, ezáltal nem kell beleegyezést kérni a felhasználásukhoz. Mindezek kitárgyalása közben feltételeztük, hogy a felhasználónk egy GDPR-t alkalmazó ország lokációjáról kereste fel a weboldalt. Ez esetben a weboldal üzemeltetője köteles a GDPR szabályozásait alkalmazni, amely esetben ezt nem tudja megtenni, le kell tiltania a bejövő forgalmat ezekről a területekről. Azonban nem mindenki ennyire szerencsés, hogy egy ilyen országba szülessen. Más országok állampolgárainak privát

szféráját nagyon kevés hasonló szabályozás védi, habár léteznek nemzetközi standardok, a weboldalak nem mindig tudnak lépést tartania az újabbnál újabb nemzeti szabályozásokkal. [11]



Ábra 1 - GDPR alkalmazásának folyamatábrája
forrás: https://ico.org.uk/media/images/other/2618969/cookies-gdpr.png

Az élmény személyre szabásának célja az ajánlások automatizálása a felhasználó eddigi érdekeltségei alapján. Ezt a jelenséget először Eli Pariser nevezte el, mint "Szűrőbuborék",[12] de manapság inkább csak "buborék" -ként említjük. A buborék egy személyre szabott keresés eredménye, ahol egy algoritmus szelektíven próbálja megjósolni, milyen információt szeretne látni a felhasználó, az általa összegyűjtött információk alapján. Bár kezdetben ez érdekes lehet, a felhasználót elszigeteli azoktól a nézőpontoktól, témáktól vagy eseményektől, amelyek nem egyeznek az eddigi felhasználói tevékenységgel, és elszigeteli a felhasználót a saját információs buborékjában.

Azonban az eredeti cél az online marketing hatékonyabbá tétele volt, hiszen ez a közösségi médiák és a big tech egyik legnagyon közvetlen bevétele. A Google például beszkenneli az összes emailünket, annak ellenére, hogy erre nem adtunk külön engedélyt, mindössze egyszer regisztrációkor elfogadtuk a felhasználási feltételeket. Ami ennél még nagyobb probléma, hogy a használt szegmentációs algoritmusok (clustering), a klasztereket, mint "unsupervised learning" saját maguk hozzák létre. Így fordulhat elő, hogy szexuális orientáció, egészségügyi állapot vagy rassz alapján mutat specifikus reklámokat az algoritmus. [13]

Egy másik sok kérdést felvető módszer a pénzügyi megbízhatóság felmérése az említett technológiák segítségével. A Lenddo nevű vállalat úgy méri a pénzügyi megbízhatóságunkat a facebook segítségével, hogy amely esetben az ismerőseink közül többen visszafizetési nehézségekkel küzdenek, úgy a mi megbízhatósági értékünket is csökkentik, mindezt annak mértékében, hogy pontosan milyen közeli kapcsolatban állunk, ami könnyen mérhető a profiljaink interakciójával. 2009-ben egy amerikai lakos kredit limitje 10800 dollárról 3800-ra csökkent egy Walmart-ban történt bevásárlás után. Az American Express azzal indokolta ezt, hogy a Walmart ügyfeleknek gyakran vannak visszafizetési nehézségeik. [14]

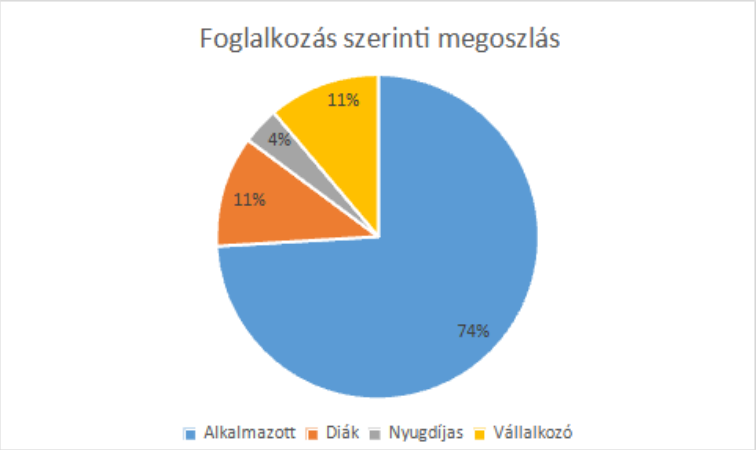
Az aktivitásunk sokat elmond az életvitelünkről és szokásainkról. Úgyhogy elsődleges célpontja olyan vállalatoknak, akiknek anyagi érdeke fűződik a fizikai állapotunkhoz. Az Allfinanz és a TCP LifeSystems olyan szoftvert fejlesztett, ami azt próbálja számolni, mekkora eséllyel kap egy felhasználó rákot vagy, hogy mikor fog balesetet szenvedni. Az ehhez szükséges adatokat a felhasználók költési előzményeiből, feliratkozásaiból szolgáltatják. Ezen adatok alapján, sűrűbb orvosi vizsgálatokat rendelhetnek el az ügyfeleiknek. [15]

Az átlagember számára azonban a legtöbbet diskurált téma a kormány adatkezelési, pontosabban adatgyűjtési szokásai és azok célja. Ebben az esetben a "Nagy Testvér mindent lát" hangok nem feltétlen vannak távol a valóságtól. Az ügynökségek pontosan ugyanazokat az ujjlenyomatozó technológiákat használják, mint a privát szektor tagjai. Az Edward Snowden által nyilvánosságra hozott dokumentumokban bizonyosságot nyer, hogy az amerikai NSA és a brit GCHQ a Google PREFID sütijeit használja az állampolgárok követésére. Ez azt is bizonyítja, hogy az NSA a privát szektor segítségével kémkedik. [16]

Biztonságtudatossági felmérés

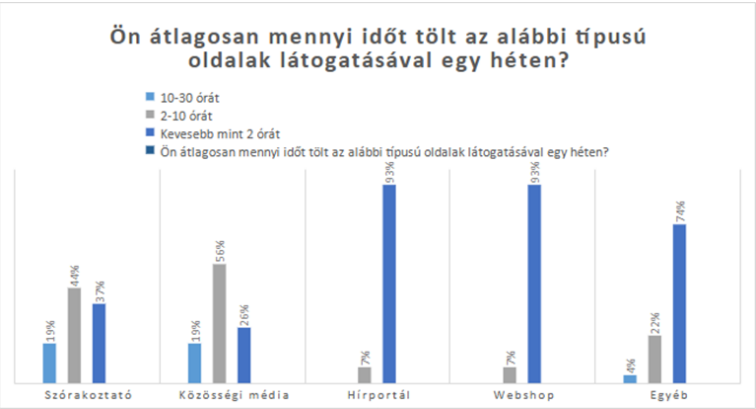
A téma vizsgálatához fontosnak tartottuk megismerni a felhasználók véleményét is a kérdésben. Ehhez egy rövid kérdőívet állítottunk össze, majd az elkészült felmérésiívet hólabda módszerrel, az ismerősi körünkben megosztva, majd őket arra kérve, hogy osszák tovább gyűjtöttük.

• Mi az ön foglalkozása? – Célunk volt, hogy a lehető legdiverzebb célközönségből vegyük a mintát.



Ábra 2 - Foglalkoztatottsági megoszlás

• Ön átlagosan mennyi időt tölt az alábbi típusú oldalak látogatásával egy héten? - A felsorolt választási lehetőségek csak látszatban egyenlő értékűek számunkra, valójában a közösségi média oldalak és a szórakoztató weboldalak, (mint például.: Netflix, Youtube) nagyobb kitettséget jelentenek az internetes nyomon követésnek és profilozásnak. Az oldalon eltöltött idővel arányosan nő az ezeken a weblapokon működő profilozó algoritmusok hatékonysága.



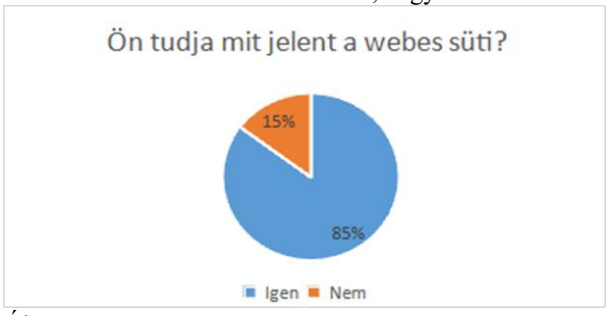
Ábra 3 - Böngészési szokások

Ön lépett-e már vissza weboldalról biztonsági megfontolásból? - Ez a kérdés a biztonságtudatosságra általánosan hivatott rákérdezni. A kérdés az "Ön mennyire tartja magát ébernek biztonságtudatossági szempontból" helyettesítése. Viszont a kitöltőnek nem kell felmérnie saját tudását, mert félő, hogy ez szubjektív lenne. Az eredményekből úgy tűnik a kitöltők 100%-a tisztában van azzal, hogy az internetnek vannak veszélyei, ezeket a veszélyeket felmérte és döntést hozott cselekvésre.



Ábra 4 – Biztonsági megfontoltságból történő visszalépés weboldalról

Ön tudja mit jelent a webes süti? - A kérdés az internetes nyomon követés alapegységének ismeretére kérdez rá. A válaszolók 85% ismeri az internetes süti fogalmát. Ez azt is jelentheti, hogy a böngészőjében használ sütiket érintő beállításokat, vagy akár rendszeresen törli a sütiket.



Ábra 5
Süti fogalmának ismerete
forrás: saját szerkesztés a kérdőívesfelmérésre kapott válaszok mintája alapján

Ön olvasott már Adatkezelési tájékoztatót? - Ez a kérdés lényegében a "Ön lépett-e már vissza weboldalról biztonsági megfontolásból?" következő szintje. A válaszadók 56%-a nem csak, biztonságtudatosan cselekedett, hanem a döntéshozatalába beépítette az adatkezelési tájékoztatót is.



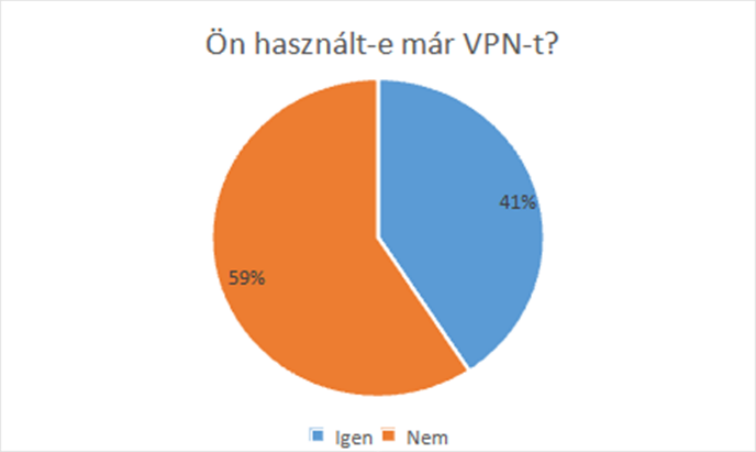
Ábra 6 – Adatkezelési tájékoztató általános ismerete

Ön esett-e már áldozatul adatlopásnak? (Pl.: bankkártyaadatok, személyes adatok) - A kérdés ismét a biztonságtudatossággal kapcsolatos. Általában összefüggés van az adatlopás és a felelőtlenség között, habár ez nem törvényszerű. A kitöltők 15% esett már áldozatul adatlopásnak, ami az eddigi eredmények fényében meglepő.



Ábra 7 – Adatlopásokkal kapcsolatos tapasztalat

Ön használt-e már VPN-t? - A kérdésben ismét egy biztonságtudatossággal kapcsolatos technológia ismeretére voltam kíváncsi. A kitöltők 41%-a használt már vpn szolgáltatást, ami a vpn szolgáltatók intenzív marketingjét tekintve meglepően alacsony. Vpn szolgáltatások elérhetőek akár ingyenes is például az opera böngészőbe építve, vagy egy vpn szolgáltatás ingyenes verziójával.



Ábra 8 – VPN használat a mintában

Összefoglalás

A felmérés alapján kijelenthető, hogy az emberek rendelkeznek tudással az internetes biztonságról és hogy ezt a tudást be is építik a mindennapos cselekedeteikbe.

A felmérés megmutatja továbbá, hogy az emberek az interneten eltöltött idejük nagy részét közösségi médián és szórakoztató weboldalakon töltik.

Ez világtrend, hiszen egy fárasztó munkanap után az átlagember kikapcsolódásra vágyik és ezt ezeken a felületen találja meg leggyorsabban és legegyszerűbben.

A magas fokú biztonságtudatosság ellenére, a közösségi médián lévő profilozástól és nyomon követestől nem védenek meg a jó döntések. A különböző interneten fellelhető veszélyek, mint például adathalászat, vírusok, átverések már beépültek a köztudatba és a társadalom sikeresen fejlesztett ki rezisztenciát ezek ellen. A következő lépésben azt kell megértetnünk a felhasználóval, hogy csak azért, mert különböző tanúsítványokkal ellátott biztonságos oldalakra látogatnak az adataik nem lesznek biztonságban.

A tracker-ek és ujjlenyomatok teljesen más fenyegetést jelentenek, mint a tradicionális veszélyforrások. A trójaiaknál és egyéb vírusoknál, amik a legnagyobb veszélyt jelentették az előző évtizedben a veszélyhelyzet legtöbbször látványos, de minimum szembetűnő. Gondoljunk csak arra, hogy rákattintunk egy fájlra egy weboldalon és pirosan felvillan a vírusírtónk, hogy veszélyforrást talált és azonnal igényli a figyelmünket. Vagy ha potenciálisan veszélyes oldalra látogatnánk az interneten a böngészőnk a teljes képernyőn egy üzenetet ír, hogy nem mehetünk tovább. A jelenleg veszélyt jelentő technológiáknál nincs semmi olyan vizuális, vagy egyéb inger, ami tudatná velünk, hogy az adataink veszélyben vannak, pedig az adataink szivárgása folyamatosan zajlik. Nem csak új kihívásokkal nézünk szembe a probléma

felismerése terén, de az adataink védelméhez is új ismereteket kell elsajátítanunk. Ennek egy része már a böngészőnkben is elintézhető. Az opcionális sütik visszautasításával, az esszenciális sütik rendszereres törlésével és a Javascript kikapcsolásával már minimalizáljuk az adataink kiszivárgását. Ismernünk kell továbbá a minden nap használt alkalmazásainkban rejlő veszélyeket is, mivel ezek ugyanúgy szivárogtatják az adatainkat, mintha az interneten böngésznénk. Erre a legbiztosabb megoldás az open-source alternatívák használata, mint pl.: a Libre office ami a Microsoft office alternatívája vagy a Signal ami helyettesítheti a Messengert vagy a WhatsApp- ot. Ez a szolgáltatás nem tárolja el az üzeneteinket a központi szerverén, csak azok folyását vezérli. Az átküldött üzenetek csak a csatorna két végét jelentő eszközön lesz dekódolva. Rengeteg feladat áll még a szakma előtt, mire a lakosság tudatossá válik az évtized kihívásaival, de az eddig legyőzött veszélyek bizalomra adnak okot a jövőre nézve.

Források

[1] International standards OHCHR and privacy in the digital age https://www.ohchr.org/en/privacy-in-the-digital-age

[2] European Convention on Human Rights https://www.echr.coe.int/documents/d/echr/Convention_ENG

[3] EUR-Lex - 32016R0679 - EN - EUR-Lex (europa.eu) https://eur-lex.europa.eu/eli/reg/2016/679/oj

[4] Carole Cadwalladr and Duncan Campbell (2019) Revealed: Facebook’s global lobbying against data privacy laws https://www.theguardian.com/technology/2019/mar/02/facebook-global-lobbying-campaign-against-data-privacy-laws-investment

[5] Laura Hautala (2020) CCPA is here: California's privacy law gives you new rights Here's everything you need to know about the new law https://www.cnet.com/news/privacy/ccpa-is-here-californias-privacy-law-gives-you-new-rights/

[6] European Parliament resolution of 20 May 2021 on the ruling of the CJEU of 16 July 2020 - Data Protection Commissioner v Facebook Ireland Limited and Maximillian Schrems (‘Schrems II’), Case C-311/18 https://www.europarl.europa.eu/doceo/document/TA-9-2021-0256_EN.html

[7] HTTP State Management Mechanism - RFC6265 https://datatracker.ietf.org/doc/html/rfc6265

[8] Using HTTP cookies https://developer.mozilla.org/en-US/docs/Web/HTTP/Cookies

[9] Marshall Brain How Internet Cookies Work https://computer.howstuffworks.com/cookie.htm

[10] Katarzyna Szymielewicz, Bill Budingtonjune (2018) The GDPR and Browser Fingerprinting: How It Changes the Game for the Sneakiest Web Trackers 2018 június 19. https://www.eff.org/deeplinks/2018/06/gdpr-and-browser-fingerprinting-how-it-changes-game-sneakiest-web-trackers

[11] ICO - Guide to the General Data Protection Regulation (GDPR) https://ico.org.uk/media/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr-1-1.pdf

[12] Eli Pariser - Beware online "filter bubbles" - TED2011 March 2011 https://www.ted.com/talks/eli_pariser_beware_online_filter_bubbles

[13] Google Privacy Policy https://policies.google.com/privacy?hl=en-US

[14] Tom Groenfeldt (2015) Lenddo Creates Credit Scores Using Social Media https://www.forbes.com/sites/tomgroenfeldt/2015/01/29/lenddo-creates-credit-scores-using-social-media/

[15] Michael Fertik, David C. Thompson (2015) The Reputation Economy: How to Optimize Your Digital Footprint in a World Where Your Reputation Is Your Most Valuable Asset January 20, 2015 ISBN:9780385347594

[16] Von Laura Poitras, Marcel Rosenbach und Holger Stark (2013) How GCHQ Monitors Germany, Israel and the EU https://www.spiegel.de/international/world/snowden-documents-show-gchq-targeted-european-and-german-politicians-a-940135.html