TDK-dolgozat

2021.

Haidekker Tamás Árpád
Budapesti Gazdasági Egyetem Külkereskedelmi Kar

Információcsere személyek és adatfelhasználók között

Exchange of information between individuals and data users

Konzulens: Dr. Zelena András Ph.D.

Kézirat lezárásának dátuma: 2021.11.08.

Tartalomjegyzék

1. Bevezetés 1
2. A Cambridge Analytica-botrány 2
3. A közösségi oldalak szerepe 5
4. Az adatfelhasználás okai 6
5. Megoldás a biztonságos adatfelhasználásra 9
6. Az óriásvállalatok felelősségvállalása 14
7. Az adatfelhasználás hatásai, következményei 18
8. Kommunikáció a felhasználó és az adatfelhasználó között 20
9. Összefoglalás 24
10. Online és szakirodalmi források 25

1. Bevezetés

A vizsgált terület, azaz az adatvédelem „problémamegoldására” keressük a választ.
A kutatásban szereplő, megtörtént adatfelhasználási botrányok alatt, mire lettek személyes adataink felhasználva, számunkra mi a tanulság ezekből, valamint mi a globális megoldás erre. A vizsgálat célja bemutatni, hogy a közösségi média platformjain történő cselekedeteinknek, digitális lábnyomainknak, milyen következményei vannak.
Minden tettünk a világhálón, egy hatalmas értékhalmaz részévé válik.
Többféleképpen értelmezhető ez a kijelentés, de esetünkben a lényege, hogy ezek a tettek adatokká válnak, melyek a legkülönfélébb célokra lesznek felhasználva. Leginkább magát az anyagiakat látják eredményként bizonyos vállalatok, de ha mélyebbre tekintünk, a rengeteg ember, azaz felhasználók által közvetített adatok, egy olyan folyamatot indítanak el, melyekből olyan meghatározó következtetések vonhatók le, amik képesek akár egy politikai választás végeredményét is befolyásolni. Utóbbi példán túl a legnagyobb marketing cégek is a bejövő adatokból építkeznek, és az alapján tudják értékelni a folyamatos visszajelzéseket. Ha konkrétabban szeretnénk rálátni ennek a folyamatnak a működésére, elég felhozni példaként akármilyen közösségi oldalt. Ott mi a saját személyes profilunkkal, a kedvünk szerint reagálhatunk adott média tartalmakra, melyek alapvetően információt tartalmaznak. Lehet ez egy videó, kép, cikk bármilyen tematikában. A hangsúly az általunk rögzített reakción van, a visszajelzésen. Csak bele kell gondolni, hogy egy ilyen reakció mekkora súllyal, de jobban mondva értékkel bírhat. Tegyük fel, egy adott személy pozitívan reagált az adott tartalomra, máris ott van a mögöttes információ, hogy ez melyik országból, melyik városból érkezett, melyek kiegészítik a demográfiai adatokat, és végül a személyes adatokat. Az utóbbin van a hangsúly. Ugyanis a személyes adatokhoz igenis hozzáférése van számos online oldalnak, de főleg a közösségi oldalaknak. Ami lényegében teljesen érthető, ugyanis regisztrációkor mi ezt elfogadtuk, hogy az oldal a mi személyes adatainkat felhasználhatja, bizonyos keretek közé szorítva. Azonban azzal védi magát jogi szempontból, hogy ez az adat harmadik fél számára semmilyen körülmények között nem fog eljutni. Ezeknek a tudatában, ha megfigyeljük, tapasztalhatjuk, hogy az esetek döntő többségében olyan tartalmak kerülnek elénk, ezeken a platformokon, amik teljességgel a mi érdeklődési körünk. Ugyanis ezek az oldalak, az adatainkból táplálkozva kialakították, hogy a mi profilunk számára milyen tartalmat kell szolgáltatni. Lényegében besorolt minket egy kategóriába. Egy kategóriába, amit saját magunk alakítottunk ki az „online lábnyomunkkal”. Természetesen ez valamilyen szintű

komfortzónát képezhet, hiszen amellett, hogy az érdekeltségi körünk „részeit” szolgáltatják felénk, szórakozást is nyújthat. De nem egészen gondolunk bele a bizonyos következményekbe. Ugyanis ezek egyértelműen célzott tartalmak felénk, amik ugyebár közel állnak a célzott hirdetésekhez. Itt vetődik fel a kérdés, hogy mikor húzzuk meg a határt, hogy mekkora mennyiségben szeretnénk, hogy az általunk átadott adatok felhasználva legyenek? Ugyanis ezek az adatok védelemre szorulnak, hisz személyes adatokról beszélünk. Addig a pontig, amíg mi saját magunk húzunk hasznot a saját adatainkból, addig él az a bizonyos komfortzóna. Azonban, ha az adataink, mondhatni üzlet részévé válnak, mások hasznára válnak, ráadásul anélkül, hogy mi ezt bármi módon észlelnénk is, az teljes mértékben kívül esik azon a bizonyos zónán. Itt jelenik meg a probléma, hogy miképpen védhetők teljes mértékben a mi személyes adataink. Valamint garanciát adhat-e az a védelem, hogy valóban nem kerülnek harmadik félhez az adataink. Ugyanis ez nem kezdetleges, kialakulóban lévő probléma, hanem a cselekmények java lényegében most történik. Arra keressük a választ, hogy az emberek személyiségének sokszínűsége adatok halmazában mérhetővé vált-e, és ha igen, mi a felénk kommunikált indok, mely elégedettségekkel tölthet el ennek tudatában.

2. A Cambridge Analytica-botrány

Kutatásom célja megválaszolni azt a kérdést, hogy vajon minden egyes ember személyisége leírható-e adatok összességével? A Cambridge Analytica-botrány helyzete volt az, amikor tényleges következményekkel járt a személyes adatokkal való visszaélés. Több tízmillió ember személyes adatai lettek felhasználva, és kiszolgáltatva a Facebook közösségi oldalon keresztül, egy harmadik fél, a Cambridge Analytica cég számára. Egy viselkedéselemző cégből váltak ki, majd 2013-tól, mint politikai konzultációs cég működtek. Ügyfeleiknek „viselkedésalapú kommunikációt” ígértek, melyet az adatbányászat és az adatkutatás új, mondhatni forradalmi módszereivel értek el. Alapvetően a Big Five elnevezésű személyiségmodellt alkalmazták. A modell öt ponton alapszik: nyitottság, lelkiismeretesség, extraverzió, barátságosság, neuroticizmus. Online, illetve telefonos kérdőívek segítségével, ezen pontok kiértékeléseivel következtetni tudtak az emberek személyiségvonásaira. A modell ilyenkor vesz egy adott választópolgárt. Annak 120 állításról kellett eldönteni, hogy az mennyire vonatkozik rá. Ezt több mint egymillió amerikai állampolgár tette meg. Ehhez pedig hozzá adták a különböző adatbrókerektől vásárolt adatokat, melyeket szintén kivetítettek a modell elemeire. Így összesítetten 220 millió amerikai állampolgárról rendelkeztek olyan alapvető személyes adatokkal mint az életkor, nem, etnikai hovatartozás, vallási nézet, anyagi

helyzet, lakhely stb. De a modell olyannyira kifinomultnak bizonyult, hogy képes volt felmérni az adott polgárokról, hogy milyen politikai beállítottságú újságot olvasnak, milyen ételt preferálnak, illetve milyen autóval közlekednek. A számok tekintetében egy emberről ötezer adatponttal rendelkeztek. Az amerikai populációt 32 személyiségtípusba sorolták, melyekből olyan részletes összefüggéseket találtak, hogy egy adott típusú zenét hallgató ember, milyen típusú parfümöt kedvel. Összesítetten így egy hatalmas adathalmazról beszélünk, ami további adatelemzést igényelt. Ezt hívjuk Big Data-nak, melynek lényege, hogy ez a méretű adatmennyiség folyamatosan bővülni képes. Ráadásul nagyon gyors adatfeldolgozással történik mindez. Akárcsak az emberek, úgy a bevitt adatok is különböznek, így az adatok változatosak. Ezek után láthatjuk ennek a fejlődő technológiai trendnek a működését. Ha egy hatalmas adatmennyiség áll rendelkezésünkre, a legrészletesebb módszerekkel vagyunk képesek a „mikrotargetálásra", azaz az egyes csoportok megkülönböztetésére, és azok személyre szabott informálására.

Ez volt a Cambridge Analytica másik fontos eszköze, valamint itt jön képbe a fő profiljuk, a politika. Ugyanis azt a bizonyos rendelkezésükre álló adathalmazt ki tudták vetíteni az Egyesült Államok térképére, azon belül a választások alappillérére, a minden államban megtalálható választókerületekre. A korábban említett, Big Five által begyűjtött személyes adatokon belül kikövetkeztethető volt számukra, hogy egy adott személy nagy valószínűséggel melyik jelöltre fogja leadni a szavazatát. Jelen esetben a 2016-os elnökválasztást nézzük, vagyis a Demokrata párt jelöltje Hillary Clinton, a Republikánus párté pedig Donald J. Trump volt. Tudni kell, hogy a Cambridge Analytica társelnöke egy bizonyos Steve Bannon volt. Ő a Breitbart nevű jobboldali konzervatív oldal vezére volt, későbbiekben pedig maga Donald J. Trump kampány menedzsere lett. Ebből nem titok, hogy a Cambridge Analytica ügyfele Trump kampánycsapata volt. Így, a céljuk egyértelműen az volt, hogy az alapvetően demokrata beállítottságúakat, illetve a Clintont preferálókat megszólítsák, és mondhatni meggyőzzék arról, hogy végül a republikánus jelöltre adják le a voksukat. Ehhez vették elő a többi kezükben lévő személyes adatmennyiséget, amivel meg tudták határozni, hogy választókerületenként a célcsoportokat, milyen tartalmakkal tudják befolyásolni. Ehhez pedig rendelkezésükre állt a mikrotargetálás. Célzott kampányanyagokat tudtak eljuttatni személyre szabottan, melyek Trump esélyeit erősítették. Itt jön képbe a korábban említett Facebook esete. A közösségi oldalon megtalálható volt egy bizonyos quiz kérdőív. A program lényege az volt, hogy annak segítségével tudhatja meg a felhasználó, hogy ő valójában milyen személyiség. A quiz adatvédelmi irányelveinek elfogadását követően, elindult a program, ami összegyűjtötte a felhasználó Facebook-on található adatait,

illetve az ismerősei nyilvánosan elérhető információit. Összesen körülbelül 305 ezer felhasználó töltötte le az applikációt, de a szétterjedt begyűjtési mechanizmusának köszönhetően, közel 87 millió ember személyes adatait szerezték meg. Ezeket az adatokat pedig eladták a Cambridge Analytica-nak. Tehát alapvetően volt egy sebezhető pont a Facebook adatvédelmi irányelveiben. Hiszen a történtekből kikövetkeztethető, hogy a tech óriás is hozzájárulhatott az említett adatvédelmi hiba keretében, hogy a célzottan tudjanak kampány anyagokat eljuttatni a bizonyos csoportoknak. Emellett a Facebook felületén lehetőség nyílik hirdetések létrehozására. Ezeket a hirdetéseket az átlagemberek is tudják oly módon szerkeszteni, hogy azok bizonyos, választható fókuszcsoportokat célozzanak meg, majd érjenek el. Ugyebár a Cambridge Analytica számára rendelkezésre állt több tízmillió felhasználóról kiterjedten az, hogy az élet számos területén mit preferál. Ezeket kihasználva, az algoritmusuk meghatározta, hogy egy bizonyos ember, a hírfolyamát görgetve olyan hirdetést kapjon, ami személyre szabottan érinti őt, és így befolyásolja a Clinton-ról, illetve Trumpról kialakított véleményét. Ugyanis, ha az algoritmus tudta, hogy egy eddig demokratákat támogató emberről van szó, akkor mindenképpen megjelenjen neki egy videó, a Clinton külügyminiszeri posztját betöltő időszak alatt, általa történt email szivárogtatásról. Ezt az ügyet az FBI a választások előtti utolsó hónapban újra elkezdte kivizsgálni, ennek tényét pedig a Cambridge Analytica algoritmusai kiterjedten elkezdték terjeszteni. Ha pedig a rendszer másik oldalát nézzük, Big Five azt is kimodellezte, hogy mely állampolgárok ellenzik a bevándorlást. Ezen személyeket pedig olyan hirdetésekkel célozták meg, hogy amennyiben Trump elnök lesz, akkor egy hatalmas falat fog felhúzni az amerikai mexikói határra. Ezzel máris szimpatikus lett számára a republikánus, így máris nagyobb eséllyel rá fog szavazni. Emellett a módszer fordított megközelítésében is nagyban érintett volt a Facebook által történt adatgyűjtés. Ugyanis, ha a Cambridge Analytica algoritmusa látta, hogy egy bizonyos felhasználó miket kedvel, miket oszt meg, azaz látta az online tevékenységüket, máris bővülni tudtak az adathalmaz bizonyos csoportjai.

Miután az többtízmillió felhasználó adatainak, harmadikfél felé történő átadása napvilágot látott, a Facebook-ot többszázmillió dolláros büntetés érte. A vezérigazgatóját Mark Zuckerberget pedig az Egyesült Államok Kongresszusának Bizottsága hallgatta ki, ahol így nyilatkozott: *"Nem mértük fel eléggé a felelősségünket, ami óriási hiba volt. Az én hibám volt"*. Donald Trump pedig megnyerte a választásokat. Itt merül fel a kérdés, hogy vajon mindez mennyiben segíthette elő végül Trump győzelmét az elnökválasztáson? Ugyanis a különböző közvéleménykutatások, előrejelzések szinte kivétel nélkül Clinton elnökké válását jósolták. Ennek ellenére, Trump olyan államokat is megnyert, melyek korábban mindig is

demokrata pártiak voltak. A botrány történéseiből is látszik, hogy egy olyan hatalmas cég, mint a Facebook sem tudta kellően megvédeni a felhasználói legszemélyesebb adatait, és kénytelen volt az adatvédelmi irányelveiket teljes mértékben átalakítani, hogy a jövőben hasonló ne fordulhasson elő. Azonban, ami a botrány lényegének keretet ad, az a Cambridge Analytica vezérigazgatójától elhangzott mondat: „*Létrehoztunk egy modellt, amellyel képesek vagyunk megjósolni az Egyesült Államok minden egyes lakójának a személyiségét.*"
Tehát jelen esetben, egyik oldalt ott van egy cég, mely esetlegesen hibázott az adatvédelmét illetően, illetve egy másik cég, ami ezt kihasználva képes adatpontok összességéből meghatározni, hogy mi magunk kik is vagyunk.

3. Közösségi oldalak szerepe

Ha a közösségi oldalak által már ekkora lehetősége van egy algoritmusnak, a rólunk alkotott kép kialakításában, elgondolkodtató, hogyha más, akár különböző eszközök által a többi általunk virtuálisan felvitt, megosztott, tárolt adatokból, vajon mennyire pontos kép születne. E mellett hozzá kell tenni, hogy maguk a tech cégek is folytatnak adatkutatást, a saját adatbázisuk számára. Több közösségi oldal már azt is figyelembe veszi, hogy a hírfolyamon megjelent tartalmakat tovább görgetjük-e, vagy megállunk annál, és pontosan mennyi ideig. Ennek oka, hogy a vállalatok is kialakítanak profilonként egy képet arról, hogy a felhasználó érdekeltségi körei hova sorolhatók be, és ennek megfelelően alakítja ki számára az algoritmus a jövőben megjelenő tartalmakat. Céljuk, hogy minél élvezetesebbé tegyék személyenként az adott oldal, alkalmazás használatát, és minél több időt töltsön el rajtuk. A másik faktor pedig a személyre szabott reklámok elhelyezése, mely nem adhat okot a meglepődésre. Például a Facebook bevételének legnagyobb részét, azaz 48%-át a reklámbevételek adják. A legnagyobb médiacégek számára sem újdonság az adatok felhasználása. Két fő célból folytatnak adatkutatást a médiaóriások, egyik az általuk gyártott produkció kialakítása. Egyes produkciós cégek, korábban írt forgatókönyveket írattatnak át mesterséges intelligencia segítségével. Ezt úgy kell értelmezni, hogy a programmal meg tudják határozni, ki a fókuszcsoportja a leforgatandó filmnek. Egy bizonyos korosztály, ami mellé körítik az aktuális kötelező trendeket, divatot, és politikailag korrekt tartalmakat, hogy etikailag is tökéletes produkció születhessen. Ezeknek a programoknak kvázi van egy vázlata, ami folyamatosan frissül, arról, hogy mik azok a legfontosabb elemek jelenleg, amiknek egy filmbe kell kerülnie. Ezeket is szintén közvéleménykutatás célzatú adatkutatással állapítják meg. A film megjelenését előzően kiadott filmelőzeteseket, melyek egy produkció

marketingjének alapvető elemei, is ezen „szabályok” és vázlatok alapján állítják össze, akárcsak az alatta bejátszott zenéket. Emellett magát a forgatást megelőző folyamatot, a produkció engedélyezését a Big Data segíti. A rendelkezésükre álló, fókuszcsoportokból begyűjtött információk által létrehozott adathalmazban lefuttatják a forgatókönyv alap elemeit, a cselekmény vázlatos fő pontjait, a Big Data algoritmusa pedig lényegében kiszámolja, hogy van-e piaca a filmnek, mekkora költségvetéssel érdemes dolgozni, illetve mekkora bevételre lehet számítani, meghatározott bemutató dátum keretében.

A másik fő célja az adatkutatásuknak, a streaming szolgáltató platformoknál figyelhető meg. A legnagyobb ilyen cég a Netflix, aki az adatvédelmi irányelveikben foglaltak szerint automatikusan gyűjti a felhasználói adatait. Begyűjti, hogy milyen készüléken vették igénybe a szolgáltatást, a felhasználó megtekintési előzményeit, keresési lekérdezéseit, valamint a nézésével töltött időt. A vállalat bizonyos adatrészeket más forrásokból is gyűjt. Például demográfiai adatokat, érdeklődésen alapuló adatokat, internetes böngészési szokásokat. Mindezek célja, hogy kialakítsa a felhasználó számára azon felületet, melyen olyan filmek, sorozatok felhozatalát kapja ajánlásul, amik az adatokból leszűrtek alapján egyértelműen az ő ízlését képezik.

4. Az adatfelhasználás okai

De a legfontosabb tényező, hogy ezt mi, mint magánszemélyek szeretnénk-e. Ugyanis az adatvédelmi szabályok lényege és célja, hogy a személyes adataink semmilyen körülmények között ne sérüljenek, de a legfontosabb, ne kerüljenek harmadik félhez. Ez pedig nem csak a mi érdekünk, hanem az egyes nagy vállalatoké is, mint a Google, Apple, Amazon, Facebook stb. Ugyanis példaként az Európai Unió által 2016-ban meghozott általános adatvédelmi rendelet szerint: „*A rendelet kulcsszerepet játszik az alapvető jogok megszilárdításában a digitális korban, és ösztönzőleg hat a kereskedelemre azáltal, hogy világosabb szabályokat vezet be a vállalkozások és a közigazgatási szervek számára a digitális egységes piacon. Az egyetlen átfogó jogszabály megszünteti a tagállamonként különböző szabályozás jellemezte széttagoltságot és a felesleges adminisztratív terheket*.” Vagyis az Európai Unió megközelítése az, hogy az állampolgáraik adatainak védelme érdekében, központosított felügyeletet biztosítanak, annak problémamentes működése érdekében. Emellett 2020 júliusáig létezett egy bizonyos „USA-EU adatvédelmi pajzs” melynek lényege a kölcsönös gazdasági digitális adatok közvetítése volt bizonyos biztonsági keretek között, azonban ezt az Unió megszüntette, és a még nagyobb szigorítást szorgalmazta. Ebből is látszik, hogy az

egyes politikai döntéshozók is érzik annak a súlyát, ha ekkora mennyiségű adattovábbításról beszélünk. Illetve, ha az EU és egy adott tagállam oszt meg egymással adatot, azt csak akkor kaphat meg egy harmadik ország, ha az a két fél között meghozott adatvédelmi szabályokat ugyanúgy betartja, valamint többszöri engedélyadás szükséges. Megfigyelhető, hogy az egyes szervezetek, gazdasági politikai egyesületek minél zártabban kezdik kezelni az állampolgárok személyes adatait. Ennek okán vehető észre a nagy tech cégek folyamatos frissítései az adatvédelmi szerződéseikben. Ugyanis ők is törekednek arra, hogy általuk semmiképpen ne történhessen, egy esetleges adatszivárgás.
Másféle megközelítés Kína helyzete, a személyes adatok tekintetében. Ugyanis a Kínai Népköztársaság szempontja az az, hogy a biztonság jegyében megfigyeli az állampolgárok online tevékenységét, és abból von le következtetéseket. Így számos elkövetett, illetve bekövetkezendő bűncselekményt ki tudnak szűrni, meg tudnak jósolni. A biztonságpolitika nagyban hozzájárul az adatvédelem kérdéséhez az egész világon. Ugyanis az elmúlt években Európában és az Egyesült Államokban is megnőtt a terrorcselekmények száma, Sok esetben a titkosszolgálati szervezetek, utólag online felületeken lefolytatott beszélgetésekben találták meg, a bizonyos elkövetők terveit. Ennek jegyében az Unión belül megkezdődött a bizonyos terror-gyanús személyek folyamatos monitorozása. Ezeket a személyeket is részben adatkutatással tudták kiszűrni. Ugyanis a használt algoritmusok ki tudják mutatni, ha egy bizonyos személy szélsőséges oldalakat, vagy ideológiákat éltető, megosztó tartalmakat néz, vagy keres rájuk. Emellett a mesterséges intelligencia e téren olyan szintre fejlődött, hogy egyes Egyesült Államokban lévő védelmi szervek azt állítják, az általuk fejlesztett gépek képesek egy esetleges terrortámadás kialakulását előre jelezni. Ennek jegyében elmondható, hogy ugyan a személyek adatvédelme prioritást élvez, de így is szükség van azok monitorozására, bizonyos kereteken belül. Utóbbi ambivalens kijelentésnek hathat. Azonban ezen dolgoznak folyamatosan az egyes országok, és azok vezetői, hogy miképpen oldható meg az adatkutatás, az adatok elemzése, majd felhasználása ténylegesen biztonságos keretek között, és ezek a folyamatok semmiképpen sem sértsék az állampolgárokat. A hangsúly pedig az etikán van. Ezeknek az intézkedéseknek etikusnak kell maradniuk, valamint be kell tartaniuk az állampolgárok általános személyi jogait. Ennek jegyében megemlítendő, a 2021-ben tervezett „photo-scan” eljárás az Apple tech cég telefonjain az Egyesült Államokban. Ennek a célja a kiskorúak bántalmazásával kapcsolatos tartalmak kiszűrése, majd azok jelentése a rendőrségnek. Minden Apple telefonnal rendelkező amerikai állampolgár fényképeit automatikusan ellenőrizné az algoritmus, és átfuttatná egy adatbázisban. Ha talál a korábban említett bűncselekménnyel kapcsolatos fájlt, azonnal jelenti a szerveknek további

intézkedés érdekében. Számos adatvédelemmel foglalkozó szakember szerint hatalmas hiba ez az intézkedés a személyes adatokkal szemben. Ugyanis nem maga az ok a helytelen. Minden ilyesfajta bűncselekmény ellen fel kell lépni. A probléma jelen esetben, ha egy cégnek szabadkezet adunk, mellyel túlságosan nagy felelősség jár. Ha lehetősége nyílik minden felhasználója személyes fényképei közé betekintést nyernie a mesterséges intelligenciája számára, az komoly negatív következményekkel járhat. Jelen korunk egyik legbefolyásosabb üzletemberének, Elon Musknak, határozott véleménye van a mesterséges intelligenciáról. „A mesterséges intelligencia sokkal veszélyesebb, mint a nukleáris fegyverkezés”

Ugyanis a korábban említett példák során, amikor az adatkutatás érintett volt, már nem csupán emberek által irányított folyamatokról van szó. Ezeket a műveleteket, algoritmusokat többségében már mesterséges intelligenciák kezelik. Ezeket, akárcsak az adatvédelmet kellő biztonsági keretek között kell kezelni. Egyértelműen problémává válna, ha ezek a mechanizmusok folyamatossá válnának, másszóval automatizálva lennének. Az az állandó teljeskörű monitorozást jelentené. Jelen helyzetben pedig nem csak a virtuális világban „otthagyott” digitális lábnyomunkról beszélünk. A telefonok, és az azokban található applikációk az esetek többségében, maguktól, automatikusan követik a mozgásunkat, tárolják majd feldolgozzák. Nem véletlen figyelhető meg, hogy egyre többször olyan értesítéseket kapunk, ami a korábban látogatott helyszínekkel kapcsolatosak. Ezek a nyomkövető mechanizmusok tanulnak, és kitérképezik az általunk bejárt területeket. Ilyenkor, nem meglepő az a jelenség, ha számos esetben bizonyos applikációk, főként közösségi kategóriájúak, a korábban érintett helyszínnel kapcsolatos hirdetést jelenít meg számunkra. Így lehet megérteni azt a körforgást, amit korábban a Cambridge Analytica is képviselt bizonyos pontokban. Még ha nem is vagyunk tudatában, de mi közlünk számos személyes adatot ezekkel a programokkal, amiket az felhasznál. Amit mi érzékelhetünk jelen helyzetben az a marketing oldala. Vegyünk példának egy kitalált vállalatot, mely ruhák értékesítésével foglalkozik. A vállalat elhelyez egy hirdetést egy közösségi oldalon, egy fókuszcsoporttal. A fókuszcsoportban szerepel az életkor, az ország, valamint a nem. Meghirdet egy női ruhakollekcióról szóló reklámot azon a közösségi oldalon, azzal a kikötéssel, hogy ő konkrétan a 18-24 év közötti Budapesten élő nőket szeretné megszólítani. A hirdetés él, közben vegyünk egy személyt, aki a helymeghatározás alapján biztosan Budapesten él, valamint nem kapcsolta ki a közösségi oldal nyomkövetési funkcióját. Az a személy jelen esetben járt egy bizonyos plázában, majd betért egy női ruhákat is áruló boltba. Ez a bolt szintén megjelenteti magát az interneten, helyszínnel együtt, hogy ő ilyen és ilyenfajta ruhákat

árul, köztük nőieket is. A személy hazamegy. Majd, ha megnyitja a telefonját a nap végén, akkor nagy valószínűséggel a hírfolyamát görgetve, szembe találja magát a vállalat hirdetésével. Ugyanis a mesterséges intelligencia összekapcsolta a személy által meglátogatott helyszínt, és az az által megosztott információt, a cég által eladni kívánt áruval. A bolt és a vállalat nem egyezik, a program mégis össze tudta kapcsolni a kettőt, majd megcélozni a személyt, az adatpontok alapján. Ez az az összefüggési rendszer az, amiből látható mekkora súllyal bír a helymeghatározási funkció bekapcsolása is. Hasonló helyzetről van szó, ha engedélyezzük a mikrofont használatát bizonyos applikációk számára. Ugyanis a telefonok mikrofonjait felhasználva, az egyes programok mögött dolgozó számítógépek képesek felismerni az általunk elhangzottakat. Ezek pedig szintén felhasználhatók különböző marketing célokra. Példaként, ha egy személy szájából többször elhangzik, hogy ő a különböző kéziórákról beszél, akkor előbb utóbb a közösségi oldalak felületén, megjelenhetnek órákkal kapcsolatos reklámanyagok.
Ugyanakkor le kell szögezni, hogy ezen példák nem minden esetben azt mutatják be, hogy ez a technológia negatív. Mivel lényegében, ha az említett marketing célba ér, és a konklúzió esetünkben a termék vásárlása lesz, akkor kölcsönös siker könyvelhető el. De itt kell feltenni a kérdést, hogy milyen áron?
Például a Cambridge Analytica esetében azt a következtetést is levonhatjuk, hogy bizonyos állampolgárok olyan hírekről vehettek így tudomást, amiről normális esetben lehet, hogy nem. Ugyanis felhozható ellenérvként, hogy az Egyesült Államokban található médiacégek többsége nem támogatta Trumpot, ennek okán főként róla volt hallható negatív információ az egyes médiumokon. A bemutatott mikrotargetálás által az információk vegyítettek lettek, tehát máshonnan is tudott informálódni az adott személy, nem csak a mainstream média által. Ha a helymeghatározást vesszük figyelembe, és tegyük fel valaki sportol, akkor nagy segítségnek tudható be, egy applikáció pontos elemzése az ő mozgásáról, majd az abból megállapított egészségügyi adatok személyre szabott közlése. A kulcsszó esetünkben a személyes.

5. Megoldás a biztonságos adatfelhasználásra

Ugyanis láthatjuk a jó oldalait is az adataink felhasználásának. Azonban a megoldás abban rejlik, hogy ez a folyamatos adatfeldolgozás az egyen személyek érdekeit, egyenként képviselje. Nem pedig egy nagy halmazként. Példával élve ezt úgy kell elképzelni, hogy egy buborékban van az adott személy középen, a buborékon belül az adatai pedig körülötte. A

személy körbe nézve bármikor tud szemezgetni az adatai között, és amikor valamelyikkel kapcsolatban neki valamire szüksége van, azt az adatot, vagy adatokat, kifelé mutatja, közvetíti a többi buborék felé, amik azokat látják, de azt nem, hogy ki van a buborékban. Ugyanis megmarad a személy inkognitója. Ugyan ő közölt adatokat, de nem lettek azok az adatok egy személlyel összekapcsolva. A megoldás véleményem szerint, az adott ember személyének, a biztonságának a megőrzésén alapszik. Így egy komfortérzetet kaphat a felhasználó is, aki bármely alkalmazást használja, tudja, hogy az ő érdeklődési köre ugyan elérhet egy bizonyos harmadik felet, de ezt úgy teszi, hogy az ő személyes adatai inkognitóban maradnak. Ez megoldást jelentene mind a magánszemélyek, mind a tech cégek, mind a kormányok számára. Természetesen ez személyes elképzelés, de ez egy esetlegesen járható út alapgondolata. Ám itt kell rátérni arra, hogy miként kerül megvédésre mindez. Itt továbbra is arról beszélünk, hogy folyamatosan megosztjuk az adatainkat, de egy kezdetleges és esetleges megoldást találtunk arra, hogy miként lehetne elkülöníteni a személyiségünkkel járó adatokat az érdeklődési köreinkkel járó adatoktól. Továbbra sincs megoldva a védelem kérdése. Ennek a megoldásának kezdőbástyáit láthatjuk a korábban felsorolt intézkedésekben. Azokban a szabályokban, törvényekben és irányelvekben, melyeket a tech cégek és a kormányok hoztak, hoznak meg. Azonban a példaként felhozott adatvédelmi pajzs felbomlása, jele annak, hogy erősen nincs egyetértés, a vezető országok között sem. Ennek okán pedig maga a rendszer sem működik, hiszen ebben az esetben egy olyan működési folyamat következik be, ami nem csak a nagy, de a kis vállalatok érdekeit sem képviseli. Mivel a globalizáció egy már-már bekövetkezett folyamat, itt a kereslet kínálat globális szintűvé nőtte ki magát. A mikrotargetálás pedig nem tudja elérni a célját, ha lényegében kontinenseken belül is különféle akadályokba ütközik. Pedig a nagyvállalatok célját a Google adatvédelmi irányelvei is kimondják: *„Az adatokat azért gyűjtjük, hogy jobb minőségű szolgáltatásokat nyújthassunk valamennyi felhasználóinknak – kezdve az alapvető dolgokkal, például annak kitalálásával, hogy milyen nyelven beszélnek, egészen a bonyolultabb kérdésekig, például, hogy milyen hirdetéseket találnak leginkább hasznosnak”* Hiszen, ha egy Egyesült Államokban lévő vásárló bármit szeretne venni, bármely kategóriában, és pont az Európai Unióban, azon belül Magyarországon lenne számára a tökéletes eladó és annak terméke, akkor nem fogják egymást „elérni”, hiszen a két fél adatvédelmi törvényei kiblokkolják egymást. Vagyis, ha csak az érdeklődési köreinket, országonként, különböző szabályozások védik, azok a tech cégek számára használhatatlanná tennék azt, ami lényegében elkerülhetetlen, az adatok jó célú felhasználását. Erre lenne esetleges megoldás, egy egyesített, konkrét szabályok és irányelvek közé elhelyezett, globális adatvédelmi

törvény. Melyet szigorúan ellenőriznének a hatóságok. Erre pedig a kezdőlépések megtörténtek, ugyanis az Európai Unió létrehozta az egyesített adatvédelmi szabályzatot a tagállamok számára: „*A 2016 májusában elfogadott adatvédelmi csomag célja, hogy felkészítse az EU országait a digitális korra. Az európaiak több mint 90%-a azt szeretné, hogy EU-szerte mindenütt ugyanazok az adatvédelmi jogok illessék meg – függetlenül attól, hol kezelik a személyes adatait."*

A felsorolt intézkedések ismeretében érdemes megemlíteni Edward Snowden véleményét ezekről, melyet a lisszaboni Web Summit-on fejtett ki egy videóhíváson Oroszországi otthonából 2019-ben. Azonban előtte vizsgáljuk meg ki is ő. Snowden az CIA-nál azaz az Egyesült Államok Központi Hírszerző Ügynökségénél dolgozott, mint számítógépes szakember. Miután magasabb pozícióba került, szembesült a ténnyel, hogy a CIA az NSA-ével, azaz a Nemzetbiztonsági Ügynökséggel karöltve, szinte a világ összes országát és annak lakóit lehallgatja valamilyen formában. Mindezt a biztonság jegyében teszik. Snowden látta, hogy pillanatok alatt képesek egy átlagember számítógépén lévő kamerát bekapcsolni, és látni azon keresztül a történéseket. Lehetőségük van a legkülönbözőbb közösségi oldalakon tárolt privát adatokhoz való hozzáféréshez. Snowdent ez annyira megdöbbentette, hogy az eset végül arra kényszerítette, hogy rendkívül bizalmas, NSA dokumentumok ellopásához, majd később internetre való feltöltéséhez vezetett. A célja ezzel az volt, hogy a világ megtudja ez zajlik a háttérben. Visszatérve Snowden véleményére a különböző szervezetek adatvédelmi intézkedéseiről. *"The problem isn't data protection,". "The problem is data collection. Regulating protection of data presumes that the collection of data in the first place was proper, that it was appropriate and that it doesn't represent a threat or danger. That it's okay to spy on your customers or your citizens so long as it never leaks, so long as only you are in control of what it is."* A probléma nem az adatvédelem A probléma az adatgyűjtés. Az adatok védelmének szabályozása feltételezi, hogy az adatgyűjtés elsősorban megfelelő volt, és nem jelent fenyegetést vagy veszélyt. Nem baj, ha kémkedsz az ügyfeleid vagy a polgárjaid ellen, amíg az soha nem szivárog ki, amíg csak te vagy az irányítója annak, hogy mi az. Tehát ahogy korábban is elemeztem, alapvetően a biztonság jegyében nem az jelenti a legnagyobb gondot, hogyha az emberek megfigyelés alatt állnak. Az adat mennyisége a probléma, és annak a biztonsága. Ha többszázmillió, akár milliárd ember adatait tárolják, és folyamatosan frissítik, mi a garancia arra, hogy ehhez nem lesz harmadik személynek hozzáférése. Az ő élő példája is tökéletes. Általa történt egy kiszivárgás. Kiszivárogtatta a világ egyik legjobban védett ügynökségének bizalmas dokumentumait. Ebből kell következtetni arra, hogy mi a következménye annak, ha ez hasonlóan megtörténik, de az átlag állampolgárok személyes

adataival. Ez az a probléma, amit nem vizsgálnak kellően. Vagyis az adatok mozgásának és elemzésének a védelme halad a teljes biztonság felé. Azonban az adatok halmazának védelme nem. Érdemes megemlíteni a 2021 október 4-én történt incidenst, a nagy Facebook leállást. A médiaóriás összesen hat és fél órán keresztül leállt, mellyel együtt a Messenger és WhatsApp üzenetküldő alkalmazás, valamint az Instagram képmegosztó platform is. Ahogy a korábbiakban szó volt róla, ezek mind többmilliárd személyes információt kezelnek. A szakértők elsőszámú aggodalma a történtekkor nem az elérhetetlen oldalakkal való elégedetlenség volt, hanem az általuk tárolt adatok kellően biztonságban vannak e. Az összeomlás óráiban pedig megjelentek az első híradások arról, hogy körülbelül másfélmilliárd felhasználó adatai szivárogtak ki. Olyan információk, mint név, lakóhely, ismerősök, email cím, telefonszám. Az adatokat pedig egyértelműen üzleti céllal szerezték meg, amit később értékesíteni tudnak. Megállapítható, hogy még ilyen hatalmas cégek esetében történő digitális leálláskor is megtörténik a hekkerek által való helyzetkihasználás. Ennek pedig az áldozatai ugyancsak a felhasználók, ismét. Látnunk kell, hogy a történtek magának a Facebooknak is kellemetlen következményeket okoztak. Az egyik nagy rivális médiacég, a Twitter, kapva az alkalmon, bejegyzést tett közzé „*Hello, literally everyone*” kijelentéssel, azaz Üdv, mindenki. Valamint a Facebook csoport vezérigazgatója Mark Zuckerberg 7 milliárd dolláros vagyonbeli veszteséget könyvelhetett el, a zuhanó részvényárak okán. Így megállapítható, hogy a tech vállalatok számára is prioritást kellene élveznie a tömeges adatok védelmének. Tehát maga a Big Data, amiből számos cég, és olykor magánszemélyek is úgymond táplálkoznak a különböző célok véghezvitelében, a Big Data nincsen kellően védve. Azzal, hogy ekkora adathalmazzal rendelkeznek a szervezetek cégek stb. mondhatni hatalomra tesznek szert. De mi is ad erőt ennek a hatalomnak? Magánszemélyek személyes adatai. Személyes információk egyénekről. A kérdés abban merül fel, hogy vajon mi ad garanciát arra, hogy a mi általunk megosztott magán információ építő jelleggel lesz felhasználva. Mert jó oldala is van ekkora adatmennyiség használatának. Ha az alapoknál elemezzük a szituációt: Ha én egy adott programnak engedélyezem, hogy kövesse azt hány kilométert futok le bizonyos idő alatt, azt ő rendszerezni tudja. Ezentúl még statisztikát is készíthet az én egészségügyi állapotomról, számításokat végezhet, tanácsokkal láthat el. Beoszthatja a napi időmet, hogy mennyi energiát fordítsak jelen esetben magára a sportra. Egy visszajelzést képes nekem szolgáltatni saját magamról. Ráadásul rengeteg időt is megspórolva. Nézzük meg ezt a példát sokkal nagyobban. Ha egy tömegközlekedési cég látja a publikusan megosztott, személyek egyenkénti mozgásterét egy adott városban, akkor messzemenő következtéseket vonhat le a használt program. Az emberek adataiból levonja a tanulságot,

hogy mekkora mennyiségű ember, mikor és merre mozog. Ezen információk függvényében tudja a legtökéletesebb vázlatot kialakítani arra, hogy bizonyos tömegközlekedési járatok, a legkülönbözőbb kategóriákra lebontva, milyen felosztásban, milyen időintervallumokban közlekedjenek. Így láthatjuk, amikor az adatok a saját célok érdekében lettek felhasználva, illetve a közjó érdekében. Emellé kell párhuzamosan lefektetni azon jelenségeket, amikor a cégek szintén ilyen méretekben elemzik az adatokat, csak éppen üzleti célok érdekében. Azonban maga a technológia már korántsem itt tart. A korábban említett Big Five személyiségmodell pont azt a tényt húzza alá, hogy nem sima adatpontokról beszélünk egyénenként. A procedúra már visszafele is működik. Azaz az adatok összekapcsolásából szinte tökéletességgel megállapítható egy ember személyisége. Valamint összefüggések állapíthatók meg bizonyos adatok között. Bizonyos környezeti hatások hatással bírnak egy emberre, ez alapvető megfigyelés. Ugyanez megállapítható adatok esetében. Ha az Amerikai Egyesült Államokon belül, veszünk egy dél-közép államot, az ott lakó emberek többségéről nagy valószínűséggel kimondható, hogy republikánus politikai nézeteket vall. Ha pedig erről a program, az adatok alapján még jobban meg szeretne győződni, elég végig futni a többi információt az elemzett illetőről, és találni olyan pontokat, amik tovább erősítik a „gyanút". Tehát már magából az egyik legalapvetőbb személyes információinkról, a lakóhelyünkről kiindulva lehet majd a későbbiekben messzemenő következtéseket levonni valakiről, szimplán úgy, hogy az adatok közötti összefüggést felismerjük. Ezt úgy kell értelmeznünk, hogy az adatkutató rendszerek, már egy olyan személyes adatunkról is képesek tudomást szerezni, amit mi egyáltalán, semmilyen formában nem osztottunk meg a virtuális térrel. Bizonyos információ morzsák hatással vannak egymásra, majd egymásra építkezve, egy nagyobb körképet alkotnak. Esetünkben egy emberről, és az ő személyiségéről.
Így a vizsgálati fókuszomba helyezem a kérdést, hogy mi a kommunikáció a külső felek részéről abban a megállapításban, hogy a mi személyes adatainkat tárolják és felhasználják? Ha megnézzük a világ bármely országát, vagy országok közötti megállapodásokat, szövetségeket, szervezeteket, akkor arra következtetésre juthatunk, hogy alapvető mechanizmusuk, a politika. Politikusok a vezető személyek, melyeket mi magunk az állampolgárok választunk meg, hogy képviseljék az általunk preferált érdekeket, valamint irányítsák azon folyamatokat, melyek elengedhetetlenek egy ország működésében. Ezen vezető személyeknek kötelességük, hogy az adott cselekedeteik következményeképpen az emberek felé is kommunikálják, a döntésük mögötti okokat. Itt kerül fókuszba az elemzett terület az adatkutatás. Ugyanis e vezető politikai erők, ha megkérdezésre kerülnek a adatfelhasználás, azon belül a személyes adatok kezelésének témájában, akkor az emberi lét

egyik legfontosabb eleme válik úgymond indokká, a biztonság. Ennek korunk egyik legjelentősebb katasztrófájának, a 2001. szeptember 11.-i terrortámadás után bevezetett intézkedések adhatnak legpontosabb példát. Ugyanis a történések megkövetelték, hogy az embereknek muszáj a biztonságérzetet biztosítani. A számos intézkedés között, egyik legkiemelendőbb, az USA repterein megtalálható ellenőrző pontok. Ezeknél az objektumoknál, a tovább haladásnál a teljes átvilágításon túl kötelező lett az ujjlenyomat vizsgálat is. Mindenki, aki az Egyesült Államok területén repülőgéppel érkezik, vagy távozik, kötelessége mindkét kezének ujjlenyomatát rögzíteni, a korábban említett NSA adatbázisának részére. Tökéletesen bemutatja a példa, az emberek számára, hogy az legszemélyesebb adataikat tárolják, és monitorozzák, azonban mindez annak a fényében történik, hogy a jövőben soha többet ne fordulhasson elő hasonló katasztrófa. Ezen intézkedés továbbfejlesztését tapasztalhatjuk ma is, szerte a világban. Nem csak magáról a terrorelhárításról van szó, hanem magáról a bűnmegelőzésről is. A biztonság mára egy olyan értékké nőtte ki magát, melyet minden eszközzel igyekeznek a kormányok saját állampolgáraik számára maradéktalanul biztosítani. A különbséget ugyanakkor látni kell egy európai ország, és Kína esete között. Míg előbbi esetében az alapvető adatainkat ugyan tárolják, de az esetek többségében csak akkor kerülnek előtérbe bizonyos személyeknek az adatai, ha arra nyomós ok adott indokot. Ennek oka főként a személyiségi jogok védelme. Utóbbi példa esetében azonban, a kínai kormányzás a teljes megfigyelést preferálja. Az egyéni online tevékenységeken túl, a közterületeken történő cselekedetet is összevetik, és az így kapott képet elemzik. Mondhatjuk, hogy így lényegében elveszett maga a személyes tér, ellenben így ki lehet jelenteni, hogy a biztonság érdekében, a rendelkezésre álló eszközök maximális kihasználtsága lett a cél. Ez pedig már az egyének összességének a döntése, hogy vállalják ezt a velejáró procedúrát, a személyes védelmük érdekében. Valamint felmerül a bizalom kérdése, amire Snowden is utalt. Mert az egyének összessége az az adatok összességét jelenti. Ugyanis így ki lehet jelenteni, hogy a személyes védelem érdekében jöttek létre ezen adathalmazok. De ennek fényében ezen adathalmazok is ugyancsak védve vannak-e. Így az intézkedések okán ez az első számú feladata a kormányzatoknak, hogy a személyes biztonság mellett, az adat biztonság is garantálva legyen.

6. Az óriásvállalatok felelősségvállalása

A vizsgálat kérdésének másik elemezni kívánt területe a nagy cégek esete. Többségében a korábban is említett technológiai vállalatok kezelik a személyes adatainkat. A Google saját

adatvédelmi szabályzata előtt olvashatjuk: *„When you use our services, you're trusting us with your information. We understand this is a big responsibility and work hard to protect your information and put you in control."* Az ő kommunikációjuk tényként közli, hogy amikor a szolgáltatásaikat igénybe vesszük, akkor mi bizalmat fektettünk abba, hogy megvédik a mi információinkat. Emellé pedig közlik, hogy tisztában vannak azzal, hogy ez egy nagy felelősség részünkről és részükről is. Azonban keményen dolgoznak azon, hogy az általunk megadott információk védve legyenek, és mi, azaz a felhasználók irányíthassanak. Alapvetően elismeri a Google a személyes adatkezelés védelmének veszélyét, és így üzeni azt a felhasználók számára, hogy ennek ismeretében ők dolgoznak ezen a problémán folyamatosan. Természetesen itt nem csak arról beszélünk, hogy a cég miként próbálja meggyőzni arról, hogy adataikkal segítség a munkájukat, hanem előtérbe helyezik azt a jelenkori szituációt, hogy veszélyben van az online térben az felhasználók által létrehozott, és általuk kezelt adathalmaz. Ennek okán következtethető, hogy az adatvédelem prioritást élvez esetükben. A közösségi média óriás Facebook a következőképpen kezdi adatkezelési szabályzatát: *„Ez a szabályzat azon információkat határozza meg, amelyeket a Facebook, az Instagram, a Messenger és a Facebook által kínált egyéb termékek és funkciók támogatása céljából kezelünk"* Ahogy utalnak is rá, a Facebook alá több különálló online platform is tartozik. Azonban ezek a közösségi oldalak, fényképmegosztó alkalmazások, illetve üzenetküldő programok, egy, közös adatbázist használnak az adatok tárolására. Tehát az adathalmaz több forrásból is begyűjti a különböző információkat rólunk. Ahogy pedig megfogalmazták, ezen termékek a mi adataink alapján működnek. Tehát közlik velünk, hogy a mi személyes adataink összessége adja a mechanizmusát, azaz az algoritmusát a Facebook-nak, és termékeinek. Így a felhasználó egy kölcsönös megállapodásként tekinthet arra, hogy ő átadja a platformnak adatait. Ha használni szeretné a közösségi oldalt, akkor annak az a feltétele, hogy személyes információinak felhasználásába beleegyezik. Az Apple adatvédelmi szabályzata így kezdődik: *„Apple's Privacy Policy describes how Apple collects, uses, and shares your personal data. In addition to this Privacy Policy, we provide data and privacy information embedded in our products and certain features that ask to use your personal information. This product-specific information is accompanied by our Data and Privacy Icon"*

A cég előre közli, amint majd szabályzatuk bemutatja, hogy pontosan hogyan gyűjti, használja és osztja meg a személyes adatainkat minden egyes termékük. Ezt pedig termékcentrikusan teszi, azaz minden produktumhoz külön adatvédelmi irányelv társul. Ennek fényében maximálisan garantálják az adatvédelmet. Vagyis a vásárlóik teljességgel

tisztában lehetnek, hogy az általuk átadott információk csak is az ő engedélyükkel kerülnek az Apple adatbázisába.

A vizsgált kérdéshez társult példák fényében megállapíthatjuk, hogy a két fő ok-okozati indok az adataink felhasználására, az a biztonság, illetve a vállalati működés segítése. Érdemes a tech cégek esetében megemlíteni a különböző üzenetküldő alkalmazások esetét is. Ugyanis ezen applikációk az életünk szerves részeivé váltak. Ennek oka nem csak az azonnali üzenetküldés lehetősége, hanem az opció, esetleges hanghívásra vagy hangüzenet küldésre. A legtökéletesebb példa az eleinte „encrypted" azaz titkosított beszélgetésről elhíresült WhatsApp esete. Azonban ezt az alkalmazást felvásárolta 2014-ben a korábban részletesen elemzett Facebook. Ennek következményeképpen szervesen átalakult a WhatsApp adatvédelmi szabályzata. Olyannyira, hogy az legnagyobb visszhangot kiváltó frissítést nem elfogadása esetén, korlátozták az applikáció jelentős funkcióit.

„We'll continue to display a notification in WhatsApp providing more information about the update and reminding those who haven't had a chance to do so to review and accept. We currently have no plans for these reminders to become persistent and to limit the functionality of the app, The new policy is about the messages you sent to businesses via WhatsApp will be shared with Facebook too. This basically means that messaging a business on WhatsApp is not the same as one-on-one chat with your friends and family. The personal chats will remain private and no one can access them as the platform is end-to-end encrypted."

Ennek értelmezése szerint, az egymás között elküldött üzenetek, képek, hangfájlok, videók többé nem tartoztak a teljes titkosítás védelme alatt, hanem egyenesen továbbításra kerültek a Facebook szervereihez. Vagyis ugyanabba a tömbösített adathalmazba kerültek, melynek veszélyei a legjelentősebbek. Nem föltől elrugaszkodott elképzelés. ha azt jelentjük ki, hogy két ember között elküldött tartalmak, egyértelmű példái a magánszférának. Ugyanis itt nem feltétlen a biztonsági tényezőkre kell gondolni, hanem ugyancsak egy ember személyes információra. Olyasfajta információcsere, amiről szó van, mely magával hordozza azon adatokat is, amik alkotó elemei egy emberi kapcsolatnak. Jelenesetben pszichológiai oldalról érdemes a szituációt megközelíteni. Ki lehet jelenteni, hogy nagy valószínűséggel az emberek többségének nem elfogadható, ha ezen adatok, egy olyan Big Data rendszerben vannak tárolva, mely nem csak gazdasági célokat szolgál, de kiberbiztonsági szempontból is megkérdőjelezhető. A WhatsApp felhasználók száma a világon összesen 2 milliárd. Ennek a hatalmas bázissal rendelkező alkalmazásnak a kommunikációja, az adatvédelmi szabályzást tekintve, pedig szintén a felhasználó irányában intézett kölcsönös megegyezés volt. Azaz, ha a letöltő elfogadja az adatok közvetítésének tényét, vagyis a frissítést, akkor továbbra is teljes

mértékben igénybe veheti az applikáció szolgáltatásait. Ebben a kategóriában megemlítendő ellenpélda a Signal alkalmazás esete. A 2014 óta működő cég leginkább az utóbbi években lett népszerű az emberek körében, főként az imént elemzett eset okán. A Signal folytatta a teljes körű titkosított üzenetküldés lehetőségét, valamint többszörösen visszajelzést kér arról, hogy valóban a telefonkészülék tulajdonosa használja-e, a rá letöltött programot. *„Signal is designed to never collect or store any sensitive information. Signal messages and calls cannot be accessed by us or other third parties because they are always end-to-end encrypted, private, and secure."* Lényegében elmondható, hogy a Signal fő kommunikációja a letöltői felé, hogy ők semmilyen esetben sem használnak föl vagy gyűjtenek bármiféle érzékeny, azaz személyes adatot. A hangsúly pedig a privátszféra, illetve a védelem szón van. Ugyanis a kettő betartása biztosítja a felhasználó egyértelmű biztonságát a tekintetben, hogy adatai a helyén vannak kezelve, ami az, hogy az egyének birtokában maradnak. Azonban meg kell jegyezni, hogy mind a WhatsApp, mind a Signal esetében az Adatvédelmi Szabályzatok külön az egyes országok vagy szervezetek törvényei szerint vannak kialakítva. Tehát különböző pontok szerint alakították ki az egyes szerződéseket. Ez is tökéletesen tükrözi az esetet, melyet korábban elemeztünk, hogy nincs teljes egyetértés az országok között az adatvédelem tekintetében. Ha pedig különválasztottuk a bizonyos országok eseteit, meg kell említeni, a Kínából származó, 2016-ban a Bytedance tech cég által kiadott TikTokot. A jelenkor egyik legnépszerűbb alkalmazásának lényege a gyorstempójú könnyen szerkeszthető videók készítése. Rohamtempóban nőtt a letöltők száma, főként a fiatalabb, tizennyolc éven aluliak körében is. Ebben az esetben, amikor is kiskorú felhasználókról beszélünk, akkor különösen nagy hangsúlyt kell fektetni a személyi jogok és adatok alapvető védelmére. A probléma ott vetődik fel az applikációval, hogy szinte teljes egészében monitorozza, és gyűjti a felhasználóiról az adatokat. Kollektivizálja mely videókat tekintettük meg, hol tettük ezt, milyen telefonról, és azon a mobilkészüléken milyen operációs rendszer található. Mindez pedig csak a jéghegy csúcsa. Mindenképpen le kell szögeznünk a tényt mindez mellé, hogy hatalmas gazdasági verseny történik Kína és az Egyesült Államok között. Utóbbi ország volt elnöke, Donald Trump, ennek okán odáig vezette a problémás szituációt, hogy egyenesen be akarta tiltani az alkalmazást az USA-ban. A volt külügyminisztere Mike Pompeo, pedig kiberbiztonsági kockázatként nevezte a TikTok működését, az országára nézve. Ezeknek a tudatában, a cég adatvédelmi szabályzatának egy része ki is tér magára a kollektív adatgyűjtési mechanizmusukra: *„We collect information when you create an account or use the Platform. We also collect information you share with us from third-party social network providers, and technical and behavioral information about your use of the Platform. We also*

collect information contained in the messages you send through our Platform and, if you grant us access, information from your phone book on your mobile device. More information about the categories and sources of information is provided below."
Lényegében tényként közlik, hogy mindaz, amit a felhasználó cselekszik az alkalmazás felületén, az rögzítésre kerül, majd továbbításra a cég adatbázisába. Emellett bármiféle információ, ami rajtunk keresztül, egy harmadik féltől, mint forrás, került be a TikTok algoritmusába, szintén átadásra kerül az adathalmazba. Kijelenthető, hogy a cég kommunikációja a letöltői felé kimondja annak a tényét, hogy a szabályzat elfogadása után mire jogosultak. A 2019-es évet 381 millió felhasználóval, míg a 2020-as évet 700 millióval zárták. Levonható a következtetés, hogy a rendkívül gyors tempóban gyarapodó felhasználókat alapvetően nem zavarják azok az adatvédelmi rések, melyek őket is érinthetik. Alapvetően nem az alkalmazással van a probléma, hanem annak biztonsági megoldásaitól. Ebben az esetben is fel kell hozni azt a felvetést, hogy mi történhet abban az esetben, ha a több százmillió felhasználó által digitálisan otthagyott személyes adat, kikerül abból a bizonyos adathalmazból. Láthattuk a példáját a Signal esetének, mely megadja a felhasználók felé azon szolgáltatásokat, melyeket elmond magáról. Mindezt úgy teszi, hogy nyíltan szabályzatba foglalva semmiféle adatot nem gyűjt. Ennek lehetősége fennáll, mint opció bármely nagy tech számára is, mint a TikTok. De érdemes megnézni az okait, hogy miért nem érdekük így tenni, és miért vállalják azon veszélyfaktort, ami ezzel jár.

7. Az adatfelhasználás hatásai, következményei.

A 2020-ban bemutatott, Netflix által gyártott The Social Dilemma című film részben körül járja ezt a témát is. Számos nagy tech cégnél dolgozott szakembert megszólaltat a film, ezen személyek nyilatkozataiból fogok idézni a továbbiakban. Egyik fő pontja a dokumentumfilmnek, a fake news-ok, azaz a hamishírek terjedése, és az abból való profitálás. A képlet egyszerű. Az emberek hajlamosak olyan hírek, információk felé érdeklődni, melyek egyértelműen kitűnnek egy hétköznapi átlagos szalagcímtől. A korábban említett online platformokon pedig egy kattintás, amikor egy adott hírt megnyitunk, az kattintásonként profitot jelenet. A dezinformálás szó okán általában a politikai szereplők juthatnak eszünkbe, ugyanis számukra az elmúlt években az egyik legerősebb kampányfegyverré vált ez a jelenség. Azonban ugyanez megfigyelhető a fiatalabb korosztályt jobban érintő, bulvárosabb hírek körében is. Itt merül fel a kérdés, hogy miképpen vehető rá, másképpen mondva, szólítható meg egy felhasználó a legkönnyebben ahhoz, hogy mindenképpen rákattintson az

adott információt magában foglaló tartalomra? A válasz az, hogy a cégeknek, azaz az algoritmusoknak, ismerniük kell a felhasználóikat, méghozzá egyenként. Ehhez segíti hozzá őket a Big Data-ból való mikrotargettálás. Eme folyamatot pedig úgy képesek ezen applikációk végrehajtani, ha adatvédelmi szabályzataikat elfogadjuk, és mint felhasználók, lényegében engedélyt adunk arra, hogy az algoritmusaikat működtető mesterséges intelligencia kiismerjen minket, az általunk átadott adatokból. Megalkot rólunk egy személyiségtípust, amiből kiindulva pozícionálni tudja a számunkra azt az érdeklődési kört, amivel meg tud bennünket szólítani. *„And that the algorithms are not objective. The algorithms are optimized for a certain definition of success. So if you can imagine a commercial enterprise building an algorithm to determine success, then it's a commercial interest. This is usually a profit. "*- Cathy O'Neil, adattudós.

Ahogy Cathy O'Neill adatkutató is mondta, magukra az algoritmusok működésére érdemes odafigyelnünk, ugyanis mindezek folyamatosan képesek tanulni és fejlődni. Ráadásul, ha ezek az algoritmusok úgy vannak elkészítve, majd későbbiekben arra vannak optimizálva, hogy sikerorientáltak legyenek, akkor már konkrétan kereskedelmi érdekről van szó. Egy profitorientált vállalat esetében pedig ezen érdek már az elején meghatározza a céljait. Mi, mint felhasználók pedig az ily módon átalakított algoritmus célkeresztjébe kerülünk. Itt kerül a megfigyelésünk fókuszába maga az emberi viselkedés, mivel ahogy korábban is szó volt róla, ezen mechanizmusok egy személyiség képet kialakítanak rólunk. Mi pedig ugyan az esetek többségében tudatlanul, de asszisztálunk mindehez.

"*We curate our lives around this perceived sense of perfection because we get rewarded in these short term signals: hearts, likes, thumbs up and we conflate that with value and we conflate it with truth. And instead, what it is is fake brittle popularity that's short term and that leaves you even more, and admit it, vacant and empty before you did it. Because that enforces you into a vicious cycle where you're like what's the next thing that I need to do now, because I need it back. Think about that compounded by two billion people and then think about how then people react to then to the perceptions of others.*" - Chamath Palihapitiya, a Social Capital vezérigazgatója

Oly szinten megalkották számunkra ezeken a közösségi platformokon a felhasználási felületet számunkra, hogy lényegében létrejött egy egyénhez, egyedien kötődő komfortzóna, melyet lényegében ízlése szerint alakíthat. Emellett, a hangsúly, az önbizalom szón van. Mert életünk célja -ezen platformokon- a tökéletes tökéletesség bemutatása, vagy annak látszatkeltése. A különböző reakció lehetőségekkel, mint a like, a szív küldése, a mosolygó fej küldése, mind saját magunk felé való visszajelzés, mellyel növelni kívánjuk az önbizalmunkat. Azonban, ha

teljességében nézzük a képet, akkor egy ilyen nagy platform esetében akár 2 milliárd felhasználóról beszélünk. Ezen emberek pedig ugyanazon ördögi kör részei, és egymásra épülve próbálnak eleget tenni saját maguknak és másoknak, a „virtuális véleményfaktor" pedig folyamatosan napról napra változik és alakul át, ahol mindig lesz egy „következő" ember, aki a felhasználó lenni szeretne. Láthatjuk a pszichológiai hatását a közösségi oldalaknak, hogy alapvetően a működési elvük is lényegében függővé teszi a felhasználókat. Így ezen felületeken az eltöltött virtuális időt folyamatosan emelni tudják, amivel egyenes arányosan növekszik az adatgyűjtés mértéke is.

"We've created a world in which online connection has become primary. Especially for younger generations. And yet, in that world, anytime two people connect, the only way it's financed is through a sneaky third person who's paying to manipulate those two people. So we've created an entire global generation of people who were raised within a context with the very meaning of communication, the very meaning of culture, is manipulation." — Jaron Lainer, informatikus és virtuális valóság úttörő.

Lényegében létrehoztak mindezzel egy generációt, akik olyan kommunikációs kontextusban nevelkedtek, ahol a kultúra jelentése egyenlő a manipulációval. Azon manipulációval, amit főként az adatgyűjtéssel, és kutatással tudtak elérni. Ugyanis miképpen ismernék, akár ezt a generációt ily módon, ha a korábbi években nem történt volna egy tudatos adatbányászat a felhasználók személyes interakcióiból.

8. Kommunikáció a felhasználó és az adatfelhasználó között

Látni kell, hogy az egész rendszer működése egymáshoz viszonyulva kölcsönösen működik. Úgy váltak olyanokká, olyan személyre szabottakká ezek az oldalak minden egyes felhasználó számára, hogy adataikat felhasználták. Ugyanakkor e nélkül az elemzett mechanizmus, és az azt működtető algoritmus nem lett volna képes egy komplett generációt „létrehozni", ahol megfigyelhetők az egyértelmű jelei annak, hogy már-már léti tényezővé vált számukra a közösségi média. Ezeknek tudatában érdemes a Cambridge Analytica helyzetére visszatérni. A botrány után számos publikáció jelent meg arról, hogy pontosan mikre alapozhatta kutatási eredményeit a cég. *„Psychographic profiling is also part of the mix, with claims for accurate prediction of personality with big data, and the potential for even greater profiling and optimisation of political adverts."* írja Vian Bakir. A pszichografikus profilozás egyértelműen ennek a mechanizmusnak a része. Mely a Big Data segítségével egy jóval nagyobb összképbe nyert betekintést, a felhasználók személyét

tekintve. Ez a folyamat pedig a korábban is említett mikrotargetálás segítségével folytatódik. *„One such empirical research strand is on algorithmic filter bubbles, where algorithms applied to online content selectively gauge what information a user wants to see based on information about the user and their digital footprints (Pariser, 2011). For instance, various studies show that rather than spreading indiscriminately through social media, conspiracies online are concentrated within the communities who already agree with them."* írja Bakir. Ennek értelmében, szegregálni képes az algoritmus a felhasználókat, és elhelyezni őket abba a csoportba, ahol az ő véleményükkel a többiek mind egy véleményen vannak. Így láthatjuk azt a körforgást, ami maguk a felhasználók, illetve az adatfelhasználók között történik. A két fél bizonyos értelemben kiegészíti egymást, és úgymond kereslet, kínálat kapcsolatba kerülnek. Mivel egy személy mindenképpen egyedi személyiséggel rendelkezik, így az a tartalom, mely számára érdekfeszítőnek jelenthető ki, egy fajta igénnyé válik. De a tartalmat szolgáltató, vagy megosztó platform, ezt önmagában nem tudja megtalálni, besorolni, majd felmutatni. Ehhez szükséges számára a bemutatott konstrukció, mely képes a személyre szabott informálásra. Lényegében egy kétoldalú kommunikáció történik, azonban a felhasználó részéről ez a párbeszéd kognitív. Mivel mi nem vagyunk tudatában annak, hogy személyes információinkat átadjuk, és ennek eredményeképpen kapunk „választ" az adatfelhasználótól, azaz attól a féltől, aki a tartalmat közvetíti felénk. Azt sem vesszük észre, hogy sajnos az esetek többségében nem a tények kerülnek elénk, hanem bizonyos irányba elmozdított információk. Másszóval mondva befolyásolva lesznek a felhasználók, az ő igényeiktől és véleményeiktől függetlenül. *„digital influence machine, consisting of technologies for surveillance, targeting, testing, and automated decision-making designed to make advertising more powerful and efficient. They argue that political and anti-democratic actors weaponise the digital influence machine by targeting selected audiences when they are most vulnerable to manipulation through three main strategies: mobilising supporters via identity threats; dividing an opponent's coalition; and leveraging influence techniques informed by behavioural science. They further argue that rather than attempting to change people's beliefs, such weaponised campaigns aim to amplify existing resentments and anxieties, raise the emotional stakes of particular issues, stir distrust among potential coalition partners, and subtly influence decisions about political behaviours"* írja Bakir. Tehát még mielőtt meglátnánk a pozitív oldalát ennek a kommunikációnak, tisztában kell lennünk annak a felénk irányuló üzleti oldalával. A korábbiakban kitértem a politikai kampányok jelenlétére a különböző közösségi oldalak hirdetéseiben való megjelenésére. Itt Bakir azt jelenti ki, hogy az algoritmusok tökéletesen kihasználják az adott társadalmi szituációkat, mint például egy

elnökválasztás az Egyesült Államokban, vagy egy népszavazás az Egyesült Királyságban. Egyértelmű megosztottságot keltenek az egyes célzott üzenetek és hirdetések a bizonyos társadalmi csoportokon belül. Olyan szintű hatalmat és erőt ad ez maguknak az online hirdetéseknek, hogy csoportosan képesek felhasználók, azaz emberek véleményét teljes mértékben megváltoztatni. Ennek oka, hogy a hirdetések mögött az a mechanizmus áll, mely kijelenthetően ismeri az adott személyt. Ahogy Bakir írásában is áll, érzelmi faktorokat képesek már megszólítani, vagyis a személyeknek személyessé alkotnak egy témát. Valamint ez a típusú manipuláció akkor is folyamatban van, amikor mondhatni a legsebezhetőbb egy ország, vagy népcsoport, egy adott témában. *„combining psychological research and data-driven targeting to identify audience's vulnerabilities is the mainstay of digital marketers, rather than an outlying technique undertaken only by rogue organisations. The proliferation of such techniques, whether or not ultimately influential on voting behaviour, is democratically problematic. As Marchal (2020) argues, being on the receiving end of psy-ops and microtargeted ads geared towards voter suppression might well affect one's sense of electoral fairness, and potentially undermine belief in the integrity of electoral processes."* Bakir általi publikáció azt írja, hogy azzal, hogy kombinálták a pszichológiai kutatásokat, az adat alapú célzott hirdetésekkel, mindezt a tökéletes való életbeli környezetbe helyezve, egyértelműen megváltoztatták a hatalmi erőviszonyokat, mind politikai, mind financiális életben. Az is lényegében megkérdőjelezhető, hogy ilyesfajta taktikák folytán, mennyire lehet igazságos egy választás eredménye. A manipuláció az elmúlt évtizedekben is látható módszernek számított az üzleti világ számos területén is, főleg a reklámiparban. Ellenben forradalminak kijelenthető a pszichográfia és adatkutatás általi manipuláció létrejötte. Hiszen esetünkben, a minket célzó, targettáló felek lényegében ismerik a személyiségünket, melynek értelmében precízen tudnak minket, a felhasználókat befolyásolni. Problémának számít, hogy nagymértékben a befolyásolást a fake news-okkal, azaz a hamis hírekkel érik el, melyekre korábban is utaltam. Ezen hamis információk velejárója, hogy a valóságtól elrugaszkodott tulajdonságaikból fakadóan kitűnnek az átlagos, sablonos tartalmakkal bíró hírek közül. Így, egyre több és több felhasználó által kerülnek megosztásra, aminek következménye az, hogy az emberek többsége tényként is fogja kezelni. Főleg abból adódóan, hogy pont abban a célzott társadalmi rétegben lesz népszerű, ahova az algoritmus az adott felhasználót besorolta, a komfortzónájában. A hamis hírek pedig kimutathatóan gyorsabban terjednek az átlagosnál, így a tartalom terjesztőjének célja egyértelműen sikerült. Ehhez pedig segítséget nyújtott a pszichográfia és az adatkutatás együttese. *„Addressing these deficiencies, Bakir et al. (2019) argue that persuasive communication, to avoid being propagandistic, should be guided by the*

principle of informed consent. This demands that three requirements be met. Firstly, sufficient information must be provided to enable informed judgments. Secondly, this information should be of a non-deceptive nature so that consent is not achieved on false premises. Thirdly, the process must not be coerced (such as through threats): rather, consent should be freely given. In short, in order to ethically persuade (rather than manipulate) people toward a particular viewpoint, the persuadee's decision should be both informed and freely chosen: each of these is disabled by deception and coercion" Bakir publikációja szerint nem szabad, hogy propaganda-szerű irányba menjen el az online informálódás. Másszóval nem a gondolkodás nélküli információ befogadás a preferálandó. A cél, hogy a tájékozottság mértéke nőjön a felhasználók körében, és annak függvényében tudjon következtetéseket levonni a tartalmakról. Bakir egy háromlépcsős megoldást dolgozott ki a probléma megoldására. Első sorban a platform, mely a tartalmakat szolgáltatja, törekedjen arra, hogy a közölt információk széleskörűek, és elegendőek a megalapozott ítéletek meghozatalához. Másodszor, az információknak nem szabad megtévesztő jellegűeknek lennie, hogy ne történhessen hamis tényeken alapuló véleménynyilvánítás. Harmadszor pedig nem lehet kikényszeríteni egy bizonyos véleményreakciót a felhasználóból, úgy mód, hogy a szolgáltatott információ fenyegetést sugallva lett közölve. Lényegében a tartalomközlésnek etikusan kell történnie, ahelyett, hogy manipuláció által érnének el hatást a felhasználóknál. A nézőpontnak önmagában az emberek által kell kialakulnia. A hangsúly a tájékozottságon, és az öntudatból való elfogadás elvén van. *„Understanding and combating deception and coercion practiced via micro-targeting in digital political campaigns is important. Not just a normative ethical claim, this is also the view of the majority of the British and American adult population. This raises the question of whether, under pressure from regulators and governments, globally dominant US social media companies have since put in place adequate measures to eliminate the risk of further psy-ops activities in digital political campaigning. The core issue is micro-targeted deception."* Bakir úgy összegezi elemzését, hogy nem magát a mikrotargetálást kell leküzdeni, hanem annak az úgy gyakorolt módját, melynek eleme a megtévesztés. Nem csupán normatív etikai állításról beszélünk. Az Egyesült Államokban, illetve az Egyesült Királyságban élő felnőtt népesség véleménye is megegyező e tekintetben. Ennek fényében fel kell tenni a kérdést, hogy elég e a kormányzatok által való nyomásgyakorlás a globálisan domináns amerikai médiacégekre? A vállalatok elegendő változtatásokat, illetve intézkedéseket e hajtottak végre a pszichológia és adatkutatás alapú megtévesztő tartalmak megosztása ellen? Fő problémának pedig a mikro célú megtévesztést nevezte a témában.

9. Összefoglalás

Összességében dolgozatomban feltártam azokat a folyamatokat, amikből megérthetjük az adatfelhasználás működését és annak veszélyeit. A Cambridge Analytica-botrány fókuszba helyezésével elemeztem a személyes adatok felhasználásának célját. A kutatás feltárta azokat a módszereket, melyek képesek a digitális világban hagyott lábnyomainkból, messzemenő következtéseket levonni. Azaz számos gazdasági, illetve politikai stratégiának a felépítését képezik ezen eszközök. Így, bemutattam a világ legnagyobb tech cégeinek érintettségét is a témában. A kutatásom kitért ezen vállalatok komplex működési elveire, melyek meghatározóan érintik a személyes adatok kezelését. Az adatvédelem súlyosságára, a különböző online biztonsági rések felsorolásával, majd tanulmányozásával mutattam rá. Munkám szerves részét képezte azon szakirodalmi, illetve online források elemzése, melyek az adatfelhasználás jövőjével foglalkoznak, és biztonságos megoldást kívánnak találni.
A hipotézisemben megfogalmazott hatás, mely felénk a felhasználók felé irányul, abban mérhető, hogy az adatfelhasználók által közvetített információk, a személyünk ismerete nélkül nem jöhettek volna létre. A kutatásom által beigazolódott a felvetés, hogy egy személy adathalmazokból leírható. Az emberi személyiség már meghatározható adatpontok által. A folyamatosan fejlődő technológia és különböző innovációk pedig elősegítik eme folyamatot. A kutatásom rávilágít arra, hogy ugyan különböző politikai és gazdasági erők törekednek az adatvédelem súlyosságára rámutatni különböző szabályzatok és törvények által. Azonban nincs meg a teljes körű garancia az információk helyén való kezelésére. A dolgozatom rámutat arra, hogy prioritást kell élveznie a személyes adataink védelmének az életünkben.

10. Online mellékletek és szakirodalomi források:

• Psychological Operations in Digital Political Campaigns: Assessing
Cambridge Analytica Psychographic Profiling and Targeting - Vian Bakir

• The Cambridge Analytica whistleblower explains how the firm used Facebook data to sway elections. Business Insider. Retrieved May 7, 2020.

• Facebook understood how dangerous the Trump-linked data firm Cambridge Analytica could be much earlier than it previously said. Here's everything that's happened until now. Gilbert, Alexandra Ma, Ben. Business Insider. Retrieved May 8, 2020.
Elon Musk Answers Your Questions! | SXSW 2018

• Bemutatjuk a céget, ami szerint miattuk győzött Trump INDEX.hu 2017.02.03. 10:36 BOLCSÓ DÁNIEL

• Big Data: A Revolution That Will Transform How We Live, Work, and Think Paperback – March 4, 2014 by Viktor Meyer Schönberger (Author), Kenneth Cukier (author)

• Cambridge Analytica staff set up a new firm BBC News. 12 July 2018. Facebook Cambridge Analytica botrány: Zuckerberg magyarázattal tartozik az európaiaknak

• The Cambridge Analytica affair and Internet-mediated research by Christophe Olivier Schneble

• Cambridge Analytica and Our Lives Inside the Surveillance Machine by Adrian Chen March 21, 2018

• Pseudo-public political speech: Democratic implications of the Cambridge Analytica scandal Published 2018 Jonathan Heawood

• https://www.portfolio.hu/uzlet/20200815/elkaszaltak-az-eu-s-adatvedelmi-pajzsot-megszolalt-az-adatvedelmi-csucsvezeto-444790

• Whatsapp, Signal, Google, Facebook, Apple, TikTok Adatvédelmi szerződései saját fordításai és magyarázata

• The Social Dilemma című Netflix filmben elhangzott bizonyos nyilatkozatok