Gradus Vol 6, No 3 (2019) 35-43
ISSN 2064-8014

# INFORMÁCIÓ = HATALOM

# INFORMATION = POWER

*Molnár Edina [1*], Bozorádi János[2]*

[1] Alapismereti és Szakmódszertani Tanszék, Pedagógusképző Kar, Neumann János Egyetem, Magyarország
[2] Szolnoki Szakképzési Centrum, Magyarország

***Kulcsszavak:***
adathalászat
manipuláció
profilalkotás

***Keywords:***
pfishing
manipulation
profiling

***Cikktörténet:***
Beérkezett 2019.07.19.
Átdolgozva 2019. 07.25.
Elfogadva 2019.08.04

***Összefoglalás***
*Mit jelent a mai világban a hatalom? Vagy a másik oldalról: hogyan képes az egyén megvédeni saját adatait, amikor minden adat a felhőben van, azaz hozzáférhető harmadik személy által. Az adatvédelem fontosságára hívja fel a cikk a figyelmet mai politikai és üzleti példák elemzésén keresztül.*

***Abstract***
*What does power mean in today's world? Or on the other side: how can an individual protect his or her data when all the data is in the cloud, ie accessible by a third party. The article calls attention to the importance of data protection by analyzing today's political and business examples.*

## 1. A net és az adatok

Információs társadalomban élünk, ahol a technikai fejlődés olyan gyors, hogy alig tudunk vele lépést tartani. Egyre intelligensebb eszközeink már a gondolatainkat is kitalálják, sőt szinte előbb tudják, mit szeretnénk, minthogy a gondolat megfogalmazódna az agyunkban. Vajon ez véletlen?

Mai modern világunkban – hála egyre gyorsabb, kényelmesebb közlekedési eszközeinknek – már nincsenek távolságok. Ha akarjuk, néhány óra alatt bárhonnan bárhová eljuthatunk. Az elektronikus információs térben pedig mindez időveszteség nélkül „online" lehetséges. Életünket „real time" módban, bárki számára megismerhetően éljük. Kapcsolataink nem korlátozódnak saját lakókörnyezetünkre, országunkra, hanem keresztül-kasul átszőhetik az egész bolygót. Ha online vagyunk, rendelhetünk árut valamelyik kedvenc kínai webáruházunkból, miközben az izlandi mitológiáról chat-elhetünk ottani barátunkkal, esetleg szétnézhetünk kedvenc közösségi portálunkon, hogy éppen milyen „live" videót oszt meg valaki a világ más szegletében. Webkamerák képeit figyelve egyszerre lehetünk jelen szinte mindenhol, és ez sokkal izgalmasabb, mint saját megszokott, sokszor unalmas vagy idegesítő környezetünk.

Ám a kibertér nyújtotta kényelemnek és izgalomnak vannak veszélyei is, melyeknek a legtöbben egyáltalán nincsenek tudatában. Amennyi lehetőséget teremt arra, hogy életünket könnyebbé, gyorsabbá, érdekesebbé és izgalmasabbá tegye, legalább annyi lehetőséget ad a visszaélésekre. Minden kattintással, minden kereséssel, minden online leütött karakterrel egyre többet fedünk fel magunkról anélkül, hogy ezt tudnánk. Agyafúrt, gyakran elfelejtett jelszavaink, tűzfalaink és vírusírtó programjaink talmi védelmében bízva gondtalanul szörfözünk a neten, intézzük hivatali és banki ügyeinket, vásárlásainkat, élvezzük, hogy a közösségi oldalakon bárkik és akárkik lehetünk – hiszen csak annyit árulunk el magunkról, amennyit mi akarunk, sőt azt mondunk, amit csak akarunk.

Csakhogy valahol az információs térben ezek az adatok mind megvannak, és aki ismeri a módját, ezeket az információmorzsákat felcsipegetve sokkal pontosabb képet kaphat rólunk, mint

* Kapcsolattartó szerző. Tel.: +36 56 510 300
E-mail cím: molnar.edina@pk.uni-neumann.hu

amit mi be mernénk vallani saját magunknak. Emellett az adatainkat nem csak mi oszthatjuk meg azokkal, akikkel akarjuk. Minden olyan információ, amit átadtunk, kikerül az ellenőrzésünk alól, és tőlünk független életet élhet, amiről lehet, hogy tudomást sem szerzünk. A bankok megosztják egymással, hogy ki a rossz vagy jó adós, a bűnüldöző szervek mára már szinte minden adattárhoz hozzáférhetnek itthon és külföldön egyaránt, kedvenc kereskedőink is megosztják partnereikkel vásárlási szokásainkra vonatkozó információikat.

Van, amikor mindez a kényelmünket szolgálja vagy segít betartani bizonyos szabályokat. Pl. e-mailt kapunk arról, hogy hamarosan lejár valamelyik okmányunk érvényességi ideje. Ugye, milyen jó, hogy emlékeztetnek erre? Vagy kedvenc divatáruházunk értesít, hogy jelentős kedvezménnyel vásárolhatjuk meg az új tavaszi kollekciót, melyhez saját bankunk készséggel biztosít nagyon olcsón áruvásárlási hitelt. Mindez mára egyszerű, magától értetődő, természetes, bár néha bosszúságot érzünk a sok levélszemét, a képernyőnkön kéretlenül megjelenő reklámok, személyre szabott ajánlatok garmadái miatt. Sokszor érzünk haragot, amikor rájövünk, manipulálni akarnak. Ilyenkor bosszúból jól leiratkozunk, majd csalódottan tudomásul vesszük, hogy ennek dacára ugyanúgy kapunk mindent továbbra is. De mi van akkor, ha nem jövünk rá a megtévesztésre?

## 2. Befolyásolás a neten

Vajon minden manipuláció annyira átlátszó, mint a szokványos marketing jelszavak: „Csak Önnek, csak most, csak ennyiért! Vigyázzon, utolsó darab!”? Van, akit ez azonnal vásárlásra ösztönöz, de legtöbben már nem dőlnek be. Emiatt mára a manipulációs technikák is egyre bonyolultabbá, több rétegűvé váltak, de mindennek az alapja az információ vagy más néven adat.

Vajon egy 16 éves, minden ősében német, hithű, katolikus családban nevelkedett lányból, aki soha egy mecsetbe be nem tette a lábát, hogyan lesz dzsihadista? Linda Wenzel Moszul ostrománál esett fogságba. Azután szökött meg kelet-németországi otthonából, hogy az interneten felvette a kapcsolatot az iszlamistákkal. Törökországon és Szírián keresztül egy hónap alatt jutott el Irakba, és feltehetően egy évet töltött el az Iszlám Államnál. Moszulban hozzáment egy dzsihadistához, akit nem sokkal később megöltek. [9] Hogyan lehetséges, hogy egy demokrata érzelmű amerikai, aki elutasítja a konzervatívok legtöbb választási célkitűzését, szavazatával mégis az ellenjelöltet támogatja?

A virtuális térben meglévő adataink összegyűjtve, rendszerezve többet árulnak el rólunk, mint hinnénk. Ezeket az adatokat személyhez kötve bárkiről minden megtudható, pl. hol él, kik a barátai, ismerősei, családos-e, milyen autómárkákat vagy sportokat szeret, ki a kedvenc zeneszerzője, de akár azt is, hogy milyen a vallási vagy politikai meggyőződése, szexuális irányultsága, stb. De hogyan lehetséges ez? Hiszen minden kereső alkalmazás vagy közösségi oldal az adatvédelem ígéretével és szolgáltatásainak biztonságosságával hiteget minket. Minden visszaélés az internetes kalózok vagy hackerek műve lenne? Egy óriási globális összeesküvés áldozatai lennénk?

Ezt ma még nagyon nehéz átlátni és eldönteni, mivel a technikai fejlődéssel egyáltalán nem tartanak lépést az új technológiák biztonságos felhasználását szolgáló hardver- és szoftverfejlesztések, a jogi keretrendszer, illetve az ezek betartását, betartatását célzó kontrollmechanizmusok. Korábban az adathalászat (pfishing) leggyakrabban valamilyen kémprogram segítségével vagy megtévesztő, „ál-weboldalon” keresztül történt. Az elkövetők általában internetes csalók voltak, akik a gyanútlan felhasználó személyes jelszavainak megszerzését követően nevében vásároltak, banki műveleteket hajtottak végre, stb. Újabban a zsarolóvírusok terjednek, melyek komplett hálózatokat képesek megbénítani vagy tönkre tenni, ha a megtámadott nem fizet.

Ám ezek társadalmi veszélyessége eltörpül a felhasználói adatok összegyűjtésén és elemzésén alapuló profilalkotás, és a felhasználói profil ismeretében a személyre szabott, tömeges manipuláció veszélyeihez képest. A közelmúlt néhány eseménye most kezdi ráirányítani a figyelmet erre a veszélyre.

A legutóbbi amerikai elnökválasztás folyamatának manipulálása már biztosra vehető. Ugyanakkor az még egyáltalán nem tudható, hogy kik és főként milyen érdekek mentén avatkoztak be a választók manipulálásával az elnökválasztás folyamatába. Már a beavatkozás ténye is alapjaiban képes megrendíteni a demokratikus intézményrendszer működésébe vetett hitet, tehát kézenfekvő a régi ellenség – az oroszok – nyakába varrni mindezt, ám az elnök kampányát vizsgáló

különleges ügyész nyomozása egy másik szálat is elkezdett felgöngyölíteni. (2017. május 18-án Rod Rosenstein, az igazságügyi tárca miniszterhelyettese jelentette be, hogy Robert Mueller volt FBI igazgató személyében különleges ügyészt nevez ki az amerikai elnökválasztási kampányba történő orosz beavatkozás kivizsgálása érdekében. [11])

2018. március 17-én tudósított először a média arról, hogy legalább 50 millió felhasználó adataival élt vissza egy adatgyűjtésre specializálódott cég, a Cambridge Analytica. [4] A cég egy kutató – a Cambridge-i Egyetemen oktató Aleksandr Kogan pszichológus professzor és idegtudós – applikációját használta fel arra, hogy mindazokról adatokat gyűjtsön, akik ezt okoseszközeikre telepítik. Az applikáció létrehozásának eredeti célja az volt, hogy a kutatók a felhasználók internet, ezen belül Facebook használó szokásait tanulmányozzák. Bár csak kb. 270.000 felhasználó telepítette az app-ot, ennek segítségével mégis legalább 50 millió felhasználó adataihoz férhettek hozzá. Azután kiderült, hogy ez a szám világszerte jóval nagyobb, és ezzel az ügy még nem ért véget. A Channel 4 elnevezésű, kereskedelmi alapon működő, de közszolgálati feladatokat is ellátó brit televíziós csatorna 2018. május 20-án tette közzé azt a felvételt, amelyben a Srí Lanka-i üzletembernek álcázott riporterük rejtett kamerájával felvette, amint Alexander Nix, a Cambridge Analytica vezérigazgatója elmondja, cége milyen lejáratő kampányokkal és módszerekkel tud hitelteleníteni politikai vagy akár üzleti riválisokat. A felvételből kiderül, hogy az amerikai elnökválasztás mellett a cég hasonló módon avatkozott be a Brexit kampányba is. A Facebooknál korábban kutatóként dolgozó Joseph Chancellor – aki korábban a Global Science Research igazgatója volt – juttatta el az adatokat a Cambridge Analytica elemzőcégnek. Miután a Facebook tudomást szerzett az adatgyűjtésről, felszólította a Cambridge Analyticát, hogy töröljenek minden adatot, az elemzőcég pedig ennek megtörténtét vissza is igazolta. Azóta kiderült: valójában nem törölték a felhasználóktól begyűjtött adatokat. A Facebook válaszként letiltotta az elemzőcég anyavállalata, a Strategic Communication Laboratories összes hozzáférését. Az SCL (Strategic Communication Laboratories) Csoporthoz tartozik a Cambridge Analytica, melyet az SCL alcégeként alapították 2013-ban, és aminek az adatgyűjtéskor és azok felhasználásakor, tehát 2014-től Steve Bannon, Donald Trump kampányfőnöke és fehér házi tanácsadója volt a vezetője. Másik cégét a Global Science Research-t (GSR) Alexander Kogan, a módszer megalkotója, a Cambridge Egyetem idegtudósa alapította.

A botrányt a Facebook igyekezett titokban tartani, ami miatt a céget alapító Mark Zuckerberg kínos magyarázkodásra kényszerült először az amerikai szenátus tényfeltáró bizottsága, majd az Európai Parlament előtt is. Zuckerberg mindenkitől bocsánatot kért, és bizonyos szigorításokat is bevezettek, melyek ugyanakkor a történtek fényében semmiféle garanciát nem jelentenek a felhasználók számára. A botrány megingatta a Facebook árfolyamát, sokan leiratkoztak és elhagyták a közösségi portált, de a vihar mára elülni látszik a cég körül. Megfelelően szabályozott jogi környezet híján komolyabb felelősségre vonásra nem lehet számítani.

## 3. Profilalkotás a bűnügyi nyomozásban

Hogyan is működik tehát a manipuláció, melynek alapja a profilalkotás? A profilalkotás – mint módszer – a bűnüldöző munka területén jelent meg először. Mai értelemben vett profilalkotásról először dr. James A. Brussel New York-i pszichiáternek egy az 1950-es évekbeli robbantássorozat kapcsán felállított elkövetői személyiségrajza kapcsán beszélhetünk, aki a nyomozás adatai alapján elkészítette az ismeretlen elkövető személyiségprofilját. E szerint a tettes Connecticut államban él, átlagos testalkatú, középkorú, külföldön született, római katolikus, nőtlen férfi, akit anyja gyötrően szeretett, apját gyűlöli, paranoiás, bátyjával vagy lánytestvérével él együtt, és amikor megtalálják, nagy valószínűséggel kétsoros, begombolt zakót fog viselni. A rendőrség később elfogta George Metesky-t, akivel kapcsolatban a pszichiáter csak abban tévedett, hogy két húgával élt együtt. Még a kétsoros zakó is stimmelt. [3]

A sorozatbűncselekmények elkövetőiről alkotott személyiségrajz támpontot ad a nyomozóknak az elkövető célirányos felkutatásához. A kriminalisztika – mint alkalmazott bűnügyi tudomány – a szociológia, a pszichológia, az antropológia és más „embertudományok” eredményeire is támaszkodva igyekszik a felkutatott bizonyítási eszközök alapján következtetéseket levonni az elkövető külső és belső személyiségjegyeire, tulajdonságaira vonatkozóan.

A helyszíni nyomok begyűjtése, azok konkrét személyhez kapcsolása már régóta segíti a bizonyítást, nélkülözhetetlen a büntetőjogi felelősség megállapítása során. A kriminalisztika résztudományágai komoly tapasztalatokat halmoztak fel a nyomok, anyagmaradványok vizsgálatával, és az azokból levonható kriminalisztikai következtetésekkel kapcsolatban. A kriminalisztikai azonosítás alapja az a ténymegállapítás, mely szerint egy személy vagy tárgy csak önmagával lehet azonos. A személy azonosítása pedig külső személyiségjegyei – testképe, egyedi személyazonosítást lehetővé tévő testi tulajdonságai – meghatározásával nagy biztonsággal elvégezhető. Végső során, ha van DNS-ünk, esetleg kéznyomtöredékünk, meg tudjuk határozni, hogy az kitől származik. De mi történik akkor, ha semmiféle tárgyi bizonyítási eszközünk nincs, vagy a meglévőket nem tudjuk konkrét személyhez kapcsolni? Ilyenkor is rengeteg információ gyűjthető be, ám a releváns információk közötti kapcsolatokat meg kell találni.

Az adatok, információk elemzése, illetve ezek alapján különböző következtetések levonása – szakkifejezéssel verziók felállítása – együtt jár a bűnüldözői munkával, de a bűnelemzés módszertanának tudományos igényű megalapozása és önálló tevékenységként történő beépítése a napi bűnüldöző munkába hazánkban csak az 1990-es évek közepétől kezdődött.

A bűnügyi szakemberek következtetéseik során logikai módszereket és eljárásokat alkalmaznak, mint az indukció, a dedukció, az analógia, az analízis-szintézis, a szelekció, az eliminációó, a kombináció stb., továbbá egyes filozófiai tételek is részét képezik a kriminalisztikai gondolkodásnak. [6] Emellett a racionális megismerésben – bármilyen furcsa – szerepet játszik az intuíció és a fantázia is. A bűnelemzői munka mindezen túl az adatok begyűjtésének, rendszerezésének, szűrésének és elemzésének módszertanával is foglalkozik. Az adatbázisok szűrése matematikai függvények alkalmazásával leegyszerűsíthető, de nagy mennyiségű adatok (pl. hívásinformációs vagy cellainformációs adatok) szűrését és rendszerezését megfelelő szoftverek nélkül csak komoly munkaerő-ráfordatással és hosszú idő alatt lehet elvégezni, melyben a hibalehetőség is nagy. Ugyancsak sok időt vesz igénybe a nyomozási iratok elemzése, amikor esetenként több ezer oldalt kell átolvasni és manuálisan kigyűjteni a releváns információkat. Ezt a munkát egyre sokoldalúbb és kifinomultabb szűrőalkalmazások segítik, ami azért vált lehetségessé, mert az adatok döntő többsége rendelkezésre áll valamilyen elektronikus adathordozón is vagy könnyen digitalizálható.

A bűnelemzés definícióját elég általánosan a rendőrség bűnelemzési szabályzata így fogalmazza meg: „az egyes bűncselekmények adatainak, a bűnügyi hírszerzés adatainak és egyes ügyek információtartalmának vizsgálatával foglalkozó tevékenység, amely segítséget nyújthat az ismeretlen elkövetők felderítéséhez, a nyomozási cselekmények tervezéséhez, a bűnöző személyek, csoportok ellen folytatott bűnüldöző munka feladatainak meghatározásához.” [12] A bűnelemző munka lényegében a nyomozás során keletkező valamennyi – tehát nyílt és titkos eszközökkel beszerzett – adat célirányos, sokszempontú elemzése. Ám ez így a legtöbb ember számára semmit sem mond, de ha megnézzük, hogy milyen részterületei vannak, sokkal érthetőbbé válik a dolog:

- ügyelemzés,
- összehasonlító ügyelemzés,
- elkövetői csoport-elemzés,
- specifikus profilelemzés.

Témánk szempontjából most ez utóbbi kettővel foglalkozunk. A profilalkotásnak több típusa létezik [1]:

- induktív profilalkotás,
- deduktív profilalkotás,
- pszichológiai profilalkotás,
- szociológiai profilalkotás,
- geográfiai profilalkotás.

Az induktív profilalkotás során a statisztikai adatok (bűnügyi, elsősorban ENyÜBS – Egységes Nyomozási, Ügyészségi, Bírósági Statisztika, mely a felfüggesztett és befejezett nyomozások, lezárt büntetőeljárások adatait tartalmazza – és ügyforgalmi adatok), az elkészült elemzések, a profilalkotó személyes tapasztalatai és a nyilvántartások adatai alapján készítik el a profilt. A deduktív módszer során az elkövető tulajdonságait gyűjtik össze, a tárgyi bizonyítási eszközök (pl. helyszíni nyomok)

és az elkövetési körülmények alapján. A geográfiai profilalkotás alapja egy számítógépes program, mely nagy valószínűséggel képes meghatározni sorozat bűncselekmények esetén az elkövető lakhelyét. A program megalkotásában azon felhalmozott tapasztalatok nyújtottak segítséget, hogy a bűncselekmények elkövetői általában mekkora távolságon belül követik el tettüket lakó-, munka- vagy tartózkodási helyükhöz viszonyítva. Minél nagyobb számú adat áll rendelkezésre, a program becslése is annál pontosabb lehet.

Az elkövető pszichológiai és szociológiai profiljának megalkotása során a helyszínen észleltekből, a tanúk által közölt információkból, esetleg szakértői véleményekből az elkövető külső megjelenésén túl pszichés, mentális állapotára, motivációjára, intelligenciájára, stb. utaló következtetéseket vonunk le, és ez alapján rajzolunk egy személyiségképet. Leegyszerűsítve például, a durva fizikai erőszakkal elkövetett élet elleni cselekmények indítéka leggyakrabban a személyes bosszú, tehát az elkövetőt a sértettel haragos viszonyban lévők között kell elsősorban keresni. A nyitott ajtó helyett az épületbe mennyezet vagy falbontás módszerével behatoló tettes esetén alacsony intellektusú, de olyan személy az emberünk, aki ezzel a módszerrel követi el általában a bűncselekményeit. Az elkövetői profil mellett sokszor válik szükségessé a sértettek közötti azonosságok alapján egy áldozati profil felállítása is, melynek célja végső soron a tervezett vagy előkészületben lévő bűncselekmények meghiúsítása, esetleg a tettes elfogása.

Ha a bűncselekményt több személy együtt valósítja meg, akkor az adatok elemzése is bonyolultabbá válik, hiszen szét kell válogatni az egyes személyekhez kapcsolódó információkat, és külön-külön kell az elkövetői profilokat létrehozni. De minél több az információ, a profil annál pontosabb lesz. A jó profil ismeretében nem csak a személy külső és belső tulajdonságai, személyes motivációi, lakóhelye határozható meg, hanem a különféle helyzetekben várható magatartása is.

## 4. Profilalkotás a net segítségével

A módszer tehát adott, hiszen a virtuális térben folyamatosan nyomokat hagyunk magunk után. A kérdés már csak az, hogy az összetartozó információkat hogyan gyűjtjük össze, és hogyan kapcsoljuk a megfelelő személyhez. Ez nem is olyan nehéz, ha az adatokhoz hozzáférünk. Hogyan is működik a profilalkotás?

1. lépés: az információk összegyűjtése.

Az internet korában óriási mennyiségű információ vált elérhetővé azáltal, hogy a net segítségével az emberek elkezdték a náluk keletkezett vagy felhalmozott adatokat megosztani egymással. Ahhoz, hogy a számunkra fontos információt megtalálhassuk, szükség volt kereső alkalmazások kifejlesztésére. Ezek kontraszelekciójának eredményeként mára már csak néhány ilyen alkalmazás, illetve az annak fejlesztésével foglalkozó cég uralja a piacot, azaz a netet. Minden információ elérhető rajtuk keresztül, de a szoftverüzemeltető cégek azt is tudják, hogy ki és milyen adathoz fért hozzá a világhálón. Emellett az otthoni informatikai eszközeink egyik legnagyobb problémája az adattárolás folyamatos kapacitáshiánya. Ennek enyhítésére találták ki azokat a felhő-szolgáltatásokat, melyek segítségével nem szükséges minden adatot saját otthoni gépünkön tárolni, hiszen a virtuális információs térben is elhelyezhetjük ezeket: kedvenc filmjeink, zenéink, családi fotóink és videóink, de akár cégadatok is vígan elférnek az információs felhőben. Az információs térben tehát minden együtt van ahhoz, hogy a profilalkotás módszerét felhasználva az egyének vagy akár tömegek véleményét alakítsuk igény szerint úgy, hogy ezzel helyi, regionális vagy akár globális folyamatokat befolyásoljunk.

Az informatikai gigacégek fejlesztéseinek és piacot uraló szoftvereiknek köszönhetően világszerte megnőtt a kényelmi szolgálatatásaikat igénybe vevők száma, így a róluk begyűjthető adatok mennyisége is. Minden cég arra törekszik, hogy ezeken a felhasználókon keresztül azokról is további adatokhoz jusson, akik nem az általuk fejlesztett szoftverkörnyezetet használják. Minden informatikai óriás szoftverkínálatában megtalálhatóak olyan üzleti célú alkalmazások, melyek a vállalatok működését segítik analitikával, piackutatással, illetve elemzéssel. Mindez óriási mennyiségű begyűjthető, és feldolgozandó adatot jelent.

2. lépés: az adatok szűrése, rendszerezése.

Ma már mindenki, aki netet használ – így e tanulmány szerzői is – különféle keresőprogramokkal és a közösségi alkalmazások keresőfunkcióinak használatával igyekszik a számára releváns tartalmakra rábukkanni. Ez általában bizonyos kulcsszavak megadásával történik.

Minél több a jól megválasztott kulcsszó, a szűrés eredményeképpen annál több releváns tartalmat érhetünk el.

2001. szeptember 11. után az amerikai Nemzetbiztonsági Ügynökség (NSA) totális elektronikai megfigyelést vezetett be, nem csak az Egyesült Államok területén, hanem globális szinten. A National Security Agency az Amerikai Egyesült Államok főként rádióelektronikai, jelhírszerzéssel foglalkozó hírszerző szervezete, az Egyesült Államok Hírszerző Közösségének az egyik legnagyobb költségvetésű és létszámú tagja, önálló nemzetbiztonsági szolgálat, mely az Amerikai Védelmi Minisztérium alárendeltségében működik. Tevékenységi körébe tartozik a külföldre irányuló rádiófelderítés tervezése, koordinálása, irányítása, beleértve az internetes forgalom ellenőrzését, valamint a hazai információbiztonság védelme, a kriptográfia, azaz a külföldi rejtjelfejtés és a hazai rejtjelzés biztonságának védelme. 1952. november 4-én hozta létre Harry S. Truman elnök, az addig a Külügyminisztérium alá tartozó rádiótechnikai felderítő szervezetek összevonásával és a Védelmi Minisztérium irányítása alá helyezésével. [7]

Az NSA gyakorlatilag mindenféle kommunikációt ellenőriz külföldön és belföldön egyaránt. Számos botrány kísérte ezt a tevékenységet, melyet minden esetben a szent céllal, a terrorizmus elleni küzdelemmel, és Amerika megvédésének indokával magyaráztak. Edward Snowden a CIA és az NSA volt alkalmazottja 2013-ban számos szigorúan titkos dokumentumot hozott nyilvánosságra, melyek leleplezték az NSA globális megfigyelési gyakorlatát, és hatalmas felháborodást váltottak ki külföldön és belföldön egyaránt. Snowden szivárogtatása adott lendületet azoknak a polgári jogi törekvéseknek, melyek eredményeképpen 2015. november 29-én hatályba lépet a USA Freedom Act törvény, mely a korábbiakhoz képest jelentősen korlátozza a hírszerző szervek megfigyelési lehetőségeit. [10]

Természetesen, ha egy óriási adatbázis bonyolult, sokszempontú szűréséről van szó, akkor speciális szűrőalkalmazás kifejlesztésére van szükség. Ezt tette Kogan professzor, de ilyen szűrőprogramok segítik a terrorelhárító szervek munkáját is.

Sokan talán azt hiszik, hogy a telefonok lehallgatását még mindig fejhallgatós, magnós, jobb esetben laptop-os emberek végzik egy lesötétített furgonban úgy, ahogyan azt a filmeken látni. Ez ma már az óriási mennyiségű eszköz és hatalmas adatforgalom miatt lehetetlen feladat lenne. A valóságban nagyteljesítményű számítógépek az összekapcsolt hálózatokon keresztül figyelik a mobil és vezetékes adatforgalmat (telefonbeszélgetéseket, SMS és más, a közösségi oldalakon megjelenő tartalmakat, e-maileket, stb.), kódfejtő alkalmazások, nyelvfelismerő és fordító szoftverek, valamint különféle szűrőprogramok segítenek elkülöníteni azokat a kommunikációs csatornákat és eszközöket, amelyeken számukra releváns tartalmak jelennek meg. Mindez automatikusan, valós időben, emberi közreműködés nélkül történik. Hogy a megfigyelés mennyire kiterjedt, mihez fér hozzá, annak csak a megfigyelést végző anyagi és technikai lehetőségei szabnak határt.

3. lépés: az adatok értékelése, elemzése.

Az összegyűjtött, megszűrt adatokat először aszerint kell vizsgálni, hogy a forrásuk mennyire megbízható, tehát az adat tényként kezelhető-e vagy hitelessége megkérdőjelezhető, mert forrása kétséges. Minél több tényt tudunk felhasználni, annál pontosabb lesz az elemzésünk eredménye, tehát következtetéseink valószínűsége is megnő.

Érthetőbben fogalmazva: közvetlenül a keresett személytől származó adatok – pl. kép, hang vagy videófelvétel – megbízhatósága jobb, mint bármely más személy róla adott leírása, esetleg a leírás alapján készült grafika, „fantomkép”. Ugyanígy egy telefon-lehallgatás során rögzített beszélgetés is pontosabb információval szolgál, mint bármely más személynek ugyanarról a beszélgetésről, de hallomásból szerzett ismeretei.

Az információs térben tehát a legjobb adat az, mely közvetlen a „megfigyelt” felhasználótól származik. Ugyanígy kell tekinteni a közösségi oldalakon megosztott tartalmakra is. Az adatok összekapcsolása és konkrét személyhez rendelése sem jelent problémát, hiszen minden „tiszta szoftver” elvégzi használójának azonosítását, bizonyos mennyiségű személyes adat (név, kor, nem, esetleg születési adatok) és e-mail cím megadását követően. A felhasználó azonosítása során az alkalmazás automatikusan hozzárendeli a felhasznált informatikai eszköz azonosítására szolgáló IP-címet is ezekhez az adatokhoz, és ezt minden alkalommal megismétli, akárhányszor olyan eszközről jelentkezünk be, melynek más az IP címe, mint a korábban rögzítettnek. Ilyenkor azonnal érkezik egy biztonsági figyelmeztetés, hogy valaki a jelszavunkkal akar belépni egy ismeretlen eszközről, és a rendszer engedélyt kér tőlünk a használatára. Mindez akár a biztonságunkat is

szolgálhatja, de ettől a pillanattól folyamatosan bővül az az adatbázis is, mely az ugyanazon felhasználóhoz köthető informatikai eszközöket tartalmazza, tehát valamennyi általa használt kommunikációs csatornát melyet a nethez igénybe vesz. A problémát azok az eszközök jelentik, melyeket több felhasználó, közösen használ. Ilyenek lehetnek az otthoni gépek, munkahelyi hálózatok, internetes kávézók munkaállomásai, stb. Ha ilyen eszközről bejelentkezve a felhasználó azonosította magát, a megfigyelése már nem jelent nehézséget. A helyszínadatok alapján a felhasználó nyomon követhető, mozgása, életmódja, szokásai, napi tevékenysége is feltérképezhető. Gondoljunk bele, hogy a tájékozódást segítő szoftverek mellett hány olyan alkalmazást használunk, mely szeretne hozzáférni a helyszín adatokhoz. A GPS-t használó vagy ahhoz kapcsolódó szoftverek mára már nem csak a navigációs programokra korlátozódnak. Az okosóránk és telefonunk a közöttük lévő kapcsolatnak köszönhetően máris térképen jeleníti meg, hogy napi edzésprogramunk során merre futottunk, kerékpároztunk, közben milyen kardio gyakorlatokat hajtottunk végre, eközben pulzusunk, vérnyomásunk hogyan változott, hány kalóriát égettünk el, stb. Ezt sokan meg is osztják magukról a neten.

Ha pedig azt is látjuk, hogy emberünk kikkel, milyen eszközökön keresztül tart kapcsolatot, a megfigyelést rájuk és eszközeikre is kiterjeszthetjük. Külön figyelemmel kísérhetjük a kiválasztott emberünket vagy az egyes eszközöket is. Alkothatunk tehát profilt a felhasználóról, de akár az eszközökről is. Amikor már elég sok felhasználóra vonatkozó adatot beszereztünk, akkor felhasználói csoportokat is létre tudunk hozni, méghozzá az általunk meghatározott szempontok alapján.

4. lépés: következtetések levonása.

Következtetéseinket a már fentebb említett logikai módszerek és eljárások segítségével vonjuk le. Ennek során egyaránt figyelembe kell venni a felhasználói profilokban megfigyelhető azonosságokat és különbözőségeket is.

A sikeres manipulációhoz pontosan ismerni kell a befolyásolandó egyén személyiségét. Az ehhez szükséges pszichológiai következtetések levonása a magatartástudomány terén felhalmozott ismeretek felhasználásával lehet a legeredményesebb. E tudományterület kutatásai célját tekintve szoros összefüggésben áll a profilalkotás módszerével. A magatartástudomány célja az emberi személyiség valamennyi – mentális, érzelmi, motivációs – tevékenységének, a magatartási minták kialakulásának, egészséges fejlődésének és zavarainak megismerése. E területek vizsgálata az egyén szintjén, annak társas kapcsolataiban, biológiai, szociológiai, pszichológiai, gazdasági és ökológiai kölcsönhatásaiban történik. [5] Azaz, ha már ismerjük az egyén mindennapi tevékenységét, érdeklődési körét, személyes kapcsolatrendszerét, szokásait, meghatározhatjuk személyiségét is. Kellő számú alany ismeretében tipizálás, csoportba rendezés is elvégezhető, hiszen nem mindegy, hogy egy személyt vagy egy csoportot, esetleg tömegeket akarunk-e befolyásolni.

A manipulációs stratégia és technikák megválasztásához szükséges azon következtetések levonása, melyek a meghatározott személyre vagy csoportra vonatkoznak. Ehhez a személyiségpszichológia nomotetikus irányzatának kutatási eredményeit használhatjuk fel [8], mely a törvényszerűségek feltárásával foglalkozik, nem az egyedi jellemzőket, hanem az általánosan működő szabályszerűségeket keresi a személyiség vonatkozásában. A nomotetikus felfogás szerint bizonyos jellemzők – például a személyiségvonások – mentén az emberek összehasonlíthatók egymással, ennek következtében lehetővé válik a személyiség mérése és az emberek egymáshoz való viszonyítása is. E törvényszerűségek alapján végezhető el az a tipizálás, mely az általunk kiválasztott csoport meghatározásához szükséges.

A Cambridge Analytica a Facebook adatbázisa alapján elkészítette a felhasználói profilokat, melyek ismeretében a saját szempontjai szerint rendezte csoportokba a felhasználókat, és vonta le azokat a következtetéseket, melyeket befolyásolásukhoz felhasználhatott.

5. lépés: befolyásolási stratégia megalkotása.

A befolyásolás vagy más szóval meggyőzés egy régi attitűd megváltoztatásának vagy egy új attitűd kialakításának a gyakorlata, ami információfeldolgozási folyamat eredménye [2]. Ez egy olyan közlési folyamat eredményeként lehetséges, melynek három fő eleme: az elvárás, az adat és a bizonyíték. Az elvárás az, amit a meggyőző fél remél, hogy a meggyőzni kívánt személy tenni fog a kommunikáció eredményeként. Az adat mindazon érveknek az összessége, melyek alátámasztják az elvárást, a bizonyíték pedig az elvárás és az adatok közötti kapcsolat igazolása [1].

Az elvárásnak nem szükségképpen kell megjelennie a közlési folyamatban. Korábbi empirikus kutatási adatok [1] azt támasztják alá, hogy a kollektivista kultúrákban – mint pl. Korea vagy Japán – az elvárások indirekt, míg az individualista kultúrákban – mint az USA vagy a Nyugat-európai országok – inkább azok direkt megfogalmazását preferálják.

A bevezetőben említett „Csak Önnek, csak most, csak ennyiért! Vigyázzon, utolsó darab!" marketinges példánál maradva tehát a "kimondatlan" elvárás, hogy most vásároljunk azért – és itt jön az adat – mert most nagyon olcsón juthatunk hozzá, majd íme a bizonyíték: "utolsó darab", tehát többé nem lesz ilyen jó lehetőségünk.

Az adat és a bizonyíték hatékonyságához a befogadó három reakciója szükséges: észlelnie kell a bizonyítékot, fel kell dolgoznia azt, és pozitívan kell értékelnie. Az érvelés hatékonyságát három tényező befolyásolja leginkább: a bizonyíték megerősítése külső forrás által; az érvelés teljessége; az érvek mennyisége. A külső forrásra való hivatkozás elősegíti az attitűd pozitív irányú változását, megerősíti a forrás hitelességét. Az érvelés teljességének – ami a pro- és kontra érvek összegyűjtését és átadását jelenti – is nagy hatása van a meggyőzés sikerességére. Az érvek optimális mennyisége változó, de általában a hétköznapi helyzetekben a több érv meggyőzőbb. [1]

Meggyőzés létrejöhet csekély erőfeszítést igénylő folyamatok és nagyobb erőfeszítést igénylő kognitív folyamatok révén is. Csekély erőfeszítést igénylő folyamat kifejezetten az érzésekre, érzelmekre vagy a heurisztikákra irányuló és/vagy azon alapuló meggyőzés, ahol ökölszabályokat használunk ítéletalkotásra, mivel ilyen esetben a befogadó mérsékelten veszi figyelembe a meggyőző üzenet tartalmát, illetve az attitűdtárgy speciális tulajdonságait.

Ezzel szemben a nagyobb erőfeszítést igénylő folyamatok esetén a befogadó az üzenet érveit alaposan megfontolja. Ilyen, nagyobb erőfeszítést igénylő feldolgozási folyamat pl. az aktív gondolkodás, mely üzenet hiányában is szélsőségesebb attitűdökhöz vezet. Ennek oka, hogy a gondolkodásunkat irányító sémák a gondolkodásunkat a séma irányába teszik elfogulttá. Az 1980-as évektől a meggyőzéssel foglalkozó kutatások két átfogó modellt alkalmaztak:

- az erőfeszítés nélküli – Heurisztikus-Szisztematikus Feldolgozási modell,
- és az aktív, erőfeszítést igénylő, a meggyőző közlés befogadásának klasszikus kettősfolyamat-modelljét, melyet Feldolgozási Valószínűségi Modell néven ismerünk. [1]

Az utóbbi centrális és perifériális feldolgozási utakat különböztet meg. A centrális úton létrejövő meggyőzés az érvek alapos megfontolásával jár, amelyhez motiváció és kognitív képesség szükséges. A perifériális úton létrejövő meggyőzés a befogadótól csekély erőfeszítést kívánó meggyőzési folyamatokra épít, mint pl. heurisztikák alkalmazása. A centrális vagy perifériális utak megjelenése mindenkor a személy motivációjának és képességének is függvénye. Amennyiben ezek jelen vannak, nagyobb a valószínűség az elaborációra, azaz az érvek megfontolására, és a centrális úton való feldolgozásra.

A Heurisztikus-Szisztematikus Feldolgozási Modellben az aktív, erőfeszítést igénylő folyamat kapta a szisztematikus feldolgozás elnevezést, míg a heurisztikus feldolgozás a csekély erőfeszítést igénylő heurisztikák alkalmazásával jár.

A heurisztikus feldolgozás esetén arra sincs feltétlen szükség, hogy az üzenetben felkínált érv valós legyen, egy érvnek látszó indoklás is elég lehet (pl. a társadalmi tudatban tényként élő általánosítás, hogy ami drága, az jó is), illetve ha egy információt gyakran hallunk, azt egy idő után tényként fogadjuk el. Általában ha egy személy nem eléggé motivált a szisztematikus feldolgozásra, vagy más tevékenység köti le a mentális kapacitását, akkor nagy valószínűséggel heurisztikus feldolgozás fog végbemenni. A heurisztikákat tartalmazó érvelések a személyek meglévő sémáira alapoznak. Ilyen például, hogy a hosszabb, több érv meggyőző; akit kedvelünk, abban megbízhatunk; a magabiztos személy biztosan tudja, hogy miről beszél, stb. [1]

A meggyőző üzenet centrális, azaz szisztematikus feldolgozása esetén egészen más a hozzáállása a befogadónak, a bizonyítékokat alaposabban megvizsgálja, ilyenkor fontos, hogy a bizonyíték közvetlenül vizsgálható-e a befogadó által; releváns-e; időben stabil-e; konzisztens-e önmagával; és elégséges-e a kérés alátámasztásához. A szubjektív befogadást tekintve fontos a meggyőzési folyamatban a bizonyíték jelentősége, valószínűsége és újszerűsége.

Az egyes személyek meggyőzéséhez tehát a személyiség ismerete mellett már csak a megfelelő módszer kiválasztása szükséges, mely mindkét modellen alapulhat. Ám ha tömegeket kívánnánk befolyásolni, akkor el kell döntenünk, hogy a tömeget alkotó egyéneket mely modell

szerint kívánom meggyőzni. Ehhez szükséges a tipizálás és a csoportba rendezés. Ezután az egyes csoportokhoz eltérő stratégia mentén kell a meggyőzést szolgáló információkat célzottan eljuttatni, ami történhet direkt vagy indirekt formában is.

Mit is tett a Cambridge Analytica? A Facebook adatbázisát megszerezve elkészítette a felhasználói profilokat, csoportba rendezte azokat, és többféle csatornán keresztül a megválasztott meggyőzési stratégiához igazodó célzott információkkal kezdte elárasztani az egyes csoportok tagjait. Ezek az információk lehettek – az adott csoport összetételének megfelelően – heurisztikus vagy szisztematikus feldolgozást igénylők. Mára bizonyítást nyert, hogy a befolyásolás érdekében a Brexit-szavazást, illetve az amerikai elnökválasztást megelőző kampányidőszakban nagy számban – szó szerint ezrével – hoztak létre ilyen információkat terjesztő weboldalakat, illetve nem valós Facebook profilokat, melyeken keresztül befolyásoló tartalmakat terjesztettek, illetve osztottak meg. Ezek egy része direkt lejáratő célzatú, más része az ellenvéleményeket hiteltelenítő információkat tartalmazott. Rengeteg félrevezető tartalmú információt, álhírt (fakenews) juttattak el célzottan a felhasználókhoz, melyek jelentős része megfélemlítő hatású volt.

A végeredményt ismerjük: a Brexit-szavazáson a kilépésre voksoltak valamivel többen, de a mai napig nincs elfogadott Brexit megállapodás Nagy-Britannia és az Európai Unió között, sőt nagyon valószínű, hogy a kilépés határidejének további hosszabbítására lesz szükség, emellett a szigetország fennállása talán legnagyobb belpolitikai válságát éli, hiszen a felerősödő skót és északír elszakadási törekvések miatt a felaprozódás veszélye fenyegeti. Az amerikai társadalom megosztottsága is jelentősen nőtt az esélytelennek tartott Donald Trump megválasztása óta, mely az ún. félidős vagy kongresszusi választások eredményeiből is látható. Ehhez nagy mértékben hozzájárul az elnök erősen megosztó személyisége is.

Hogy mindennek milyen hatásai lesznek a jövő alakulására, nehezen megjósolható, de az adatvédelem szükségességét feltétlenül igazolni látszik, valahogy úgy, mint ahogy a hippy korszak és a szabad szerelem virágzásának végéhez az AIDS megjelenése is hozzájárult.

## Irodalomjegyzék


[1] Balázs K. – Bernáth Á. (2015) A viselkedés befolyásolására alkalmas kommunikációs módszerek. In Kovács J. (szerk.) Szociálpszichológiai tanulmányok a Szociál- és Munkapszichológiai Tanszék fennállásának 25. évfordulójára, 207–229. Debreceni Egyetemi Kiadó

[2] Chaiken, S., Wood, W., Eagly, A. H. (1996) Principles of persuasion. In E. T. Higgins & A. W. Kruglanski (Eds.), Social psychology: Handbook of basic principles, 702-742. New York, NY, US: Guilford Press.

[3] Gampel Andrea – Székely György László (2009) A profilalkotás alkalmazásának lehetőségei a magyar büntetőeljárásban. Ügyészek Lapja XVI. Különszám, 22–23.

[4] HVG. hu (2018) 40-50 millió Facebook-felhasználó érintett, rengeteg a károsult a most kirobbant adatgyűjtési ügyben. http://hvg.hu/tudomany/20180317_cambridge_analytica_adatgyujtes_facebook

[5] Kopp Mária – Skrabski Árpád (2009) Magyar lelkiállapot az ezredforduló után. Távlatok/86, 32-52. http://www.tavlatok.hu/86/86kopp_skrabski.pdf

[6] Lakatos János (szerk.) (2005) Kriminalisztikai alapismeretek. Budapest, Rendőrtiszti Főiskola

[7] National Security Agency. https://www.nsa.gov

[8] Oláh Attila – Gyöngyösiné Kiss Enikő (2007) A személyiség fogalma és vizsgálati módszerei: mérés, kutatás, elmélet. In: Gyöngyösiné Kiss Enikő, Oláh Attila (szerk.) (2007) Vázlatok a személyiségről – a személyiség-lélektan alapvető irányzatainak tükrében. Budapest, Új Mandátum Könyvkiadó https://www.researchgate.net/profile/Eniko_Kiss/publication/260248443_A_szemelyiseg_fogalma_vizsgalati_modszerei_meres_kutatas_elmelet/links/0deec53050ae3b0360000000.pdf

[9] The Guardian (2017) German girl imprisoned for Isis role has fleeting family reunion. https://www.theguardian.com/world/2017/dec/15/german-girl-linda-wenzel-imprisoned-for-isis-role-has-fleeting-family-reunion

[10] The Guardian (2013) NSA files: decoded. https://www.theguardian.com/world/interactive/2013/nov/01/snowden-nsa-files-surveillance-revelations-decoded#section/1

[11] The Guardian (2019) Special counsel Robert Mueller's testimony postponed by one week. https://www.theguardian.com/us-news/2019/jul/12/special-counsel-robert-mueller-congress-testimony-postponed

[12] A Magyar Köztársaság Rendőrsége Bűnelemzési Szabályzatának kiadásáról szóló 13/2001. (X. 2.) ORFK utasítás