Iványi Márton

Megtévesztés, színlelt attitűd és a közösségi média

A közösségi médiában előfordul, hogy valaki megkísérli elrejteni felhasználói profiljának egyes információit annak érdekében, hogy másokat megtévesszen, másnak vagy másként mutatkozzon meg, mint aki valójában, vagy egyszerűen csak új arculatot épít – ez természetesen áttételesen a megosztásokat is érinti. Mindez a legártatlanabb dolgoktól, mint a közvetlen családtagok elől a felhasználót „rossz" színben feltüntető, mulatós képeknek a „customize" (testre szabott) funkciók útján történő elrejtésétől a nagy nyilvánosság előtt a valóságos politikai napirendek képmutató leplezésén át a trójai falóként álcázott, „zoknibábok" képében jelentkező titkosszolgálati megfigyelésig terjed. A megtévesztés – amint azt e tanulmány evolúciós pszichológiai összefüggései sejtetik – a természetben gyökerezik, ezáltal mindennapjaink része. A közösségi média inherens „arctalansága" folytán azok a nem verbális jelzések, amelyek adott esetben segíthetnének feltárni a megtévesztésre irányuló szándékokat, természetszerűen a háttérben maradnak.

Közösségi média és megtévesztés – definíciós kérdések

A hálózati alapú technológiák villámgyors elterjedése forradalmasította annak módját, ahogyan a tartalom keletkezik és kicserélődik a világhálón, ami a közösségi média alkalmazásainak és szolgáltatásainak robbanásszerű növekedéséhez vezetett – így hangozna a modernista-technológia narratíva empirikus tapasztalatokkal is védhető felütése.

A közösségi média elnagyolt gyűjtőfogalma és kategóriái alatt Andreas M. Kaplan és Michael Haenlein (2011) nyomán egy sor olyan internetalapú közösségi alkalmazást és szolgáltatást értünk, amelyek valójában egymástól gyökeresen eltérő virtuális környezetek. Ezek az alkalmazások és szolgáltatások teszik lehetővé a felhasználó által előállított tartalmak létrehozásának és az internetes alkalmazások tervezésének széles körét.

Ezt a növekedést nemcsak a szolgáltatások számának emelkedése táplálja, hanem a felhasználók általi átvételük gyors üteme is. Joanna Brenner és Aaron Smith (2013) szerint 2005 és 2013 között majdnem kétharmadával nőtt a közösségi média alkalmazásait használók tábora. Shen Xuemin (2013) arra a következtetésre jut, hogy például a Twitter használata tíz százalékkal nőtt 2010 és 2013 között, és jóval egymilliárd fölött jár azok száma, akik felhasználói fiókkal rendelkeznek a Facebook és a Twitter által.

Ugyanakkor a felhasználói profil létrehozásának egyszerűsége annak az esélyét is megteremti, hogy az emberek megtévesszék egymást. A megtévesztést vizsgáló kutatások megállapítják, hogy az emberek általában napi rendszerességgel hazudnak, és a múltban számos erőfeszítést tettek a megtévesztés azonosítására és a jelenség megértésére (Madhusudan 2003). Az amerikai pszichológus Paul Ekman (2010: 22) következtetése, amelyet az amerikai társadalmi tapasztalatok tükrében, vonatkozó hétköznapi példák áttekintése után von le, így szól: „A hazugság olyan központi jellemzője az életnek, hogy jobb megértése nélkülözhetetlen csaknem minden típusú emberi kapcsolat esetén."

Mielőtt továbbmennénk, érdemes áttekinteni a szóban forgó, szemantikailag rokon *megtévesztés* és *hazugság* fogalmak és kapcsolódó igéik meghatározásait.

A *Magyar nyelv szótára* (1865) a 'megtéveszt' igét a következőképpen definiálja: 'eszközli vagy okot, alkalmat ad rá, hogy valaki megtévedjen'. Például: 'A sokfelé menő utak megtévesztik a vidékkel ismeretlen utast.' 'Álokokkal megtéveszteni valakit.' A *Magyar Értelmező Kéziszótár Diákoknak* (2010: 536) szerint megtévesztésről akkor beszélünk,

ha 'valaki (vagy valami) tévedésbe ejt, félrevezet valakit'. Például: 'Megtévesztette a bírákat naiv, ártatlan viselkedésével.' 'Az tévesztette meg, hogy egy, az enyémhez hasonló kocsi állt a ház előtt.' A *Kommunikációtudományi Nyitott Enciklopédia* vonatkozó definíciója értelmében 'a hazugság egy szándékolt ellentét állítás és meggyőződés között.' A *Magyar Értelmező Kéziszótár Diákoknak* (2010: 310) a 'hazudik' igét úgy határozza meg, mint '1. Szántszándékkal valótlant állít, füllent. Például: Szemérmetlenül hazudik. Egy szavadat sem hiszem, tudom, hogy hazudsz! 2. (választékos) Színlel. boldogságot, jókedvet hazudik, pedig nagyon el van keseredve.'

Ekman (2010) a hazugságot úgy definiálná, mint olyan akaratlagos választást, amely a célpont félrevezetésére irányul anélkül, hogy erre felhívnák a figyelmét. A hazugságnak két fő formáját különbözteti meg: a leplezést, vagyis a valós információk kihagyását, illetve a hamisítást, azaz a hamis információk igazként való feltüntetését. Ám léteznek a hazugság további módjai is: a félrevezetés, egy érzelem elismerése a valós okok elkendőzésével, az igazság hamis előadása, illetve az igazság beismerése olyan túlzó vagy humoros módon, hogy a célpont továbbra sem jut többletinformációhoz, vagy félre lesz vezetve. Beszélhetünk továbbá a félig leplezett igazságról, illetve az igazság részleteinek beismeréséről, ezáltal eltérítve a célpontot az elfedett tényezőkről, illetve a hamis következtetést eredményező kitérésről, valamint az igazság oly módon történő előadásáról, amely az elhangzottak ellenkezőjére utal. Elgondolkodtató Ekman értelmezése, aki magát a megtévesztést a hazugság lepleződésének szövegkörnyezetéhez kapcsolja. A megtévesztésnek két formája van: a szivárgás, amikor a hazug akaratán kívül leleplezi az igazságot, illetve a megtévesztés jelei, amikor a hazug viselkedése utal rá, hogy amit mond, nem igaz.

A történelem során a megtévesztést különféle összefüggésekben alkalmazták a technológiával egyetemben (második világháború, Trója és Buda ostroma stb.), taktikai előnyszerzés céljából. A közösségi média új környezetet és technológiát biztosít mindehhez. Gyakran találkozni az ilyen alkalmazások és szolgáltatások szférájában a megtévesztés példáival, amelyek némely esetekben egyenesen pusztító következményekkel járnak az áldozatra nézve.

Michail Tsikerdekis és Sherali Zeadally tanulmánya (2014) a megtévesztést olyan szándékos cselekedetnek tekinti, amely arra irányul, hogy félrevezessen másokat, akik nincsenek tudatában annak, hogy egy ilyen eset éppen bekövetkezik, a cél pedig az, hogy tévhit keletkezzen a megtévesztett személyben. A szerzőpáros továbbá azt állítja Sean L. Humpherys és társai (2011) nyomán, hogy ezek a keletkező tévhitek verbális és non-verbális kommunikáció útján közvetíttetnek.

A továbbiakban a szerzőpáros által felállított modellre támaszkodva mutatjuk be a megtévesztés fogalmát és fedezzük fel annak gyakorlatait, motivációit a közösségi médiában. Számos vonatkozó technikát azonosítunk, illetve érintőlegesen az általuk kiváltott hatást is megvizsgáljuk. Miközben az azonosítás és a megakadályozás fontos, a megtévesztéssel összefüggő aspektusok, az online megtévesztés megértése és a technikák osztályozása az első lépés az ellene való küzdelemben.

Megtévesztés és természet: egy evolúciós pszichológiai perspektíva

A természet pártfogolja a megtévesztést mint stratégiai előny szerzésére szolgáló mechanizmust. A mimikri és az álcázás különböző válfajai (például a krüpszisz, avagy a vizuális, a szaglási és a hallási álcázásra való képesség, vagy a mimészisz, más szóval az utánzás), a tetszhalott állapot, a leplezés, az úgynevezett deimatikus viselkedés mind-mind az etológia által jól ismert formája a rossz információ, a félrevezető tájékoztatás állatok közötti átadásának, amelynek révén „valótlan hiedelem" terjed, és amely a populációkra jellemző kognitív képességeknek megfelelően tudatos.

Az evolúció során a mimikri az adaptáció azon formáját, eredményét jelöli, amikor egy élőlény felveszi vagy utánozza egy másik élőlény vagy a környezet mintáját, színét, külalakját, szagát, viselkedését. A megtévesztő alkalmazkodás célja lehet önvédelem; ilyen eset az álcázás, más néven kamuflázs, ami a környezetbe való beolvadást jelenti. Az önvédelem másik módja a Mertens-féle mimikri, amikor az élőlény egy másik, veszélyes élőlény külsejét ölti fel, így riasztva el a rá nézve fenyegető ellenfeleket. Az alkirály pillangók például a madarak jelentette fenyegetést azzal hárítják el, hogy a (keserű ízű) uralkodó pillangókkal egyformán néznek ki, ezáltal biztosítva fajuk fennmaradását is, egészen a túlszaporodásig. Fordított helyzetre is találunk példát: a megtévesztés másik lehetséges célja a zsákmány sikeres megközelítése, aminek egy válfaja a Peckham-féle vagy agresszív mimikri. Ilyenkor a ragadozó a zsákmányfajtához vagy egy arra veszélytelen élőlényfajtához válik hasonlóvá (tulajdonképpen „báránybőrbe bújt farkas").

Az alkalmazkodás aktív formájának a sebessége változatos lehet. A polip egyetlen másodperc alatt képes a terep színéhez, mintázatához igazodni, míg más élőlények egy új terepen való huzamosabb tartózkodás esetén igazítják a külsejüket a környezethez. Az evolúciós mimikri viszont számos generáción át formálódik, és a fajta végül a természetes szelekció elve alapján éri el az olykor megdöbbentően tökéletes hasonulást. Az evolúciós mimikri is változhat az egyed élete folyamán; példa erre a rejtőszín cseréje az évszaknak, az időszaki növényzetnek megfelelően, illetve a változó életkor, életmód szerinti rejtőszín viselése.

Néhány állat taktikai megtévesztést gyakorolhat, vagyis a többi állat által félreérthető viselkedést vethet be saját előnyére. Az erre vonatkozó bizonyítékok egy része ugyan anekdotikus, mindenesetre az emberszabású majmok esetében kísérleti vizsgálatok utalnak arra, hogy a megtévesztés elterjedt egyes állatok körében.

Hasonlóképpen az ember is él a megtévesztéssel, jó- vagy rosszindulatú szándék által vezérelve (Burgoon et al. 2005), bár nehezebb dolga van: az emberi megtévesztés mérhető és azonosítható a szóbeli (például hangok, szövegek), a nem szóban kifejezett (testbeszéd) és a fiziológiai jelek (szívverés) által, legalábbis az „offline" valóságban.

> „A hazugságok leggyakrabban azért lepleződnek le, mivel kiszivárog valamilyen rejtett érzelemre utaló jel. Minél erősebbek ezek az érzelmek […], annál valószínűbb, hogy valamilyen viselkedésbeli »kiszivárogtatás« elárulja a jelenlétüket"

– jellemzi a lelepleződés pszichoszomatikus folyamatait Ekman (2009: 20), aki szerint a félrevezetés leghatékonyabb módja egy másik, hamis érzelem kimutatása, és a leggyakoribb maszk maga a mosoly, a legtöbb ember számára a legnehezebb feladatot pedig a negatív érzelmek hamisítása jelenti.

Persze a fiziológiai jelek nem törvényszerűen fedik fel a megtévesztőt; ahogy Dosztojevszkij (1975: 97) írja az öreg Karamazovról:

> „Akik végigszínészkedték egész életüket, vannak perceik, amikor annyira beleélik magukat a szerepükbe, hogy már valóban remegnek és sírnak a felindulástól, noha még abban a pillanatban is (vagy legfeljebb egy másodperccel később) azt súghatnák maguknak: hiszen te hazudsz, [...] most is színészkedel."

Az említett árulkodó „offline" jelek evolúciós pszichológiai perspektíváját illetően Darwin (1872/1963) gyermekeken, elmebetegeken és főemlősökön végzett megfigyeléseire, valamint etnográfiai adatgyűjtésére támaszkodva arra a következtetésre jutott, hogy a nem verbális kommunikáció társas kapcsolatok szabályozását szolgáló formái – az emberi arckifejezések éppúgy, mint a gesztusok vagy a testtartások – fokozatosan alakultak ki a főemlősök jelzéseiből, ennélfogva egyetemes jellegűek az egész Földön (úgynevezett viselkedési univerzálék), és veleszületett képességeken alapulnak.

Darwin hipotézisét az 1970-es évektől kezdve meginduló kutatások nagyrészt alátámasztották, amennyiben több ízben (például Ekman & Friesen 1975, Ekman 1994), ráadásul kultúraközi összehasonlító vizsgálatok keretében megállapították, hogy a Föld bármely lakója lényegében ugyanúgy fejezi ki és érti meg az olyan alapvető érzelmeket, mint az öröm, a meglepetés, a harag vagy a szomorúság. A nem verbális jelzések lehetővé teszik, hogy az egyének közöljék társaikkal belső állapotaikat, szándékaikat, érzelmeiket stb. Az etológusok kimutatták, hogy az élőlények információkat cserélnek egymással, amelyeket legtöbbször a nem verbális jelzések, sajátos magatartásformák közvetítenek. A természetes szelekció az üzenetközvetítés hatékony, egyértelmű és informatív formáit hozta létre az élővilágban, amelyek adaptíve előnyösek a résztvevők számára. A jelzést kibocsátó fél (a továbbiakban: „adó") számára azért, mert reakciókészségének és szándékának közlésével képes megváltoztatni a másik viselkedését. Az üzenet fogadója (a továbbiakban: „vevő") viszont abból húz hasznot, hogy a rendelkezésre álló információ révén képes megjósolni az adó várható viselkedését és e viselkedés valószínű kimenetelét. Ezeket őszinte, megbízható jelzéseknek tartjuk, amennyiben a valóságos belső állapotot és szándékot fejezik ki, és mindkét fél számára kifizetődőek (Bereczkei 2003).

Ha azonban érdekeink úgy kívánják, élünk a megtévesztő kifejezések eszköztárával. Richard Dawkins és John Krebs (1978) híres, sokat idézett tanulmányában elsőként vetette fel, hogy a természetes szelekció bizonyos körülmények között olyan félrevezető jelzéseket részesít előnyben, amelyek célja a másik élőlény kihasználása, manipulálása. A jelzést adó élőlény sokszor nem az őszinte, megbízható információ küldésében érdekelt, hanem abban, hogy becsapja a vevőt. Saját hasznát – túlélését, szaporodási sikerét – ugyanis úgy növeli, hogy akkor bocsát ki jelzéseket, amikor azok a saját érdekét szolgálják, illetve olyan jelzéseket hoz létre, amelyek a saját érdekét szolgálják (Andrews 2002). Az ilyen nem kooperatív szignálokra nagyon sok, kísérletileg alátámasztott esetet ismerünk, kezdve a taktikai megtévesztés fenti példáitól a táplálékállatok tőrbecsalásán át (példa erre a horgászhal) a párzási küzdelmekig, amelyek során a hímek igyekeznek olyan eltúlzott jelzéseket adni, amelyek által nő az esélyük egyrészt arra, hogy elijesszék vagy félrevezessék a riválisa hímeket, másrészt arra, hogy felkeltsék a nőstények figyelmét. Úgy tűnik, fajunk különösen alkalmas a megtévesztő jelzések létrehozására, amelyek megkönnyítik a hazugságot és mások manipulálását (Bereczkei 2003).

Konklúzióm tehát egyfelől az, hogy a félrevezetés – amint azt a fentebb érintett vizsgálatok mutatják – a természetben gyökerezik, ezáltal a mindennapok része, ahogy különben az a közösségi média is. Másfelől az, hogy az utóbbi használata során– miként ezt majd látni fogjuk a felállított adó-tartalom-csatorna-vevő modell prizmáján át – a háttérben maradnak azon nem verbális jelzések, amelyek adott esetben segíthetnének felfedni a megtévesztésre irányuló szándékokat.

Az online megtévesztés

A világhálón történő megtévesztés és manipuláció ismert jelenség. Ennek alátámasztására elég, ha arra gondolunk, hogy a kibertér a nagyhatalmak úgynevezett multispektrum-háborújának (Nazemroaya, 2014) egyik színtere, és felidézzük Szun-ce (1963) szavait is: „Minden hadviselés megtévesztésen alapul." Ahogy a „Youtube-háború" fogalma is toposszá vált a közelmúltban, különösen Szíria és Ukrajna vonatkozásában. Jelen tanulmány azonban konkrétan a közösségi médiára összpontosít, és úgymond a „civil élet" kontextusában kíván maradni.

A közösségi média szolgáltatásai a társadalmi jelenlét/információgazdagság és az önmegjelenítés/önleleplezés (a fogalmakról bővebben lásd lentebb) mátrixviszonyai alapján osztályozhatóak (Kaplan & Haenlein 2010). A *társadalmi jelenlétet* befolyásolhatja annak a médiumnak az intimitása és közvetlensége, amely magát a kommunikációt közvetíti, az *információgazdagság* pedig Richard L. Daft és Robert H. Lengel (1984) elmélete alapján arra utal, hogy milyen mennyiségű információ továbbítható az egyes médiumok által egy adott időpontban (például telefonon kevesebb, mint videokonferencia keretében ugyanabban az időintervallumban). Az *önmegjelenítés* annak a felhasználók általi szabályozását határozza meg, hogy miként képviselik önmagukat, míg az *önleleplezés* arra utal, ha valaki akarva vagy akaratlanul felfedi a saját információit.

A felhasználók számára saját maguk bemutatása és megjelenítése terén a szabadság magas fokát biztosító közösségi médiatípusok a blogok, a mikrobloggoló felületek (például a Twitter) és a közösségi oldalak (például a Facebook), a virtuális világok vagy más néven a nagyon sokszereplős online világok (Second Life, Kaneva, Onverse stb.). Más közösségi médiatípusok, mint az együttműködési projektek (például Wikipédia, Diigo), a közösségi híroldalak (például Reddit, Digg, Propeller), az online multimédiás tartalmakat megosztó közösségek (Youtube, FlickR, SlideShare) és a virtuális játékvilágok (World of Warcraft) a felhasználókra bizonyos szerepek vagy funkciók felvételét, illetve betöltését róják, vagy éppenséggel nem teszik lehetővé személyazonosságuk közzétételét. Az információgazdagság és a társadalmi jelenlét növekedésével megfigyelhető az átmenet a kizárólag a szövegalapú kommunikációt lehetővé tevő média, illetve a szóbeli és a nem verbális üzenetek révén a valódi világ szimulációjára törekvő média között, csakúgy, mint a közvetlenebb kommunikáció a virtuális (játék)világok tekintetében.

A közösségi médiaszolgáltatások e fenti különbségei magától értetődően kihatnak a megtévesztés menetére és esetleges sikerére is. A legtöbb online közösségi hálózaton a kommunikáció szövegalapú, és aszinkron történik. Ilyen környezetben a megtévesztők előnyben vannak a tartalom megváltoztatását illetően, ami a félrevezetés egy könnyű módszere. A főként a páva- és a fregattmadár-populációk tapasztalataira támaszkodva kidolgozott, úgynevezett hátrányelvmodell hipotéziséről *(handicap hypothesis)* ismert izraeli evolúciós biológus, Amotz Zahavi (1993) különbséget mutatott ki a megbízható, nehezen hamisítható, úgynevezett értékelési szignálok *(assessment*

signals) és a könnyebben hamisítható egyezményes szignálok *(conventional signals)* között. Ha például a valódi világban egy idősebb személy fiatalabbnak akar mutatkozni, megteheti, hogy fiatalosabban öltözik, befesti a haját stb., ezáltal egyezményes szignálokat adva. Azonban sokkal nehezebb dolga lenne akkor, ha történetesen a járművezetői engedélyét hamisítaná meg (értékelési szignálok). A közösségi média ugyanakkor olyan környezetet biztosít, amelyben nincs szükség értékelési jelekre, továbbá azok nem normaerejűek, ami megkönnyíti a megtévesztést. Például az online közösségi hálózatokon a nem megváltoztatásához elegendő akár a név változtatása is.

Nem meglepő, hogy az online megtévesztés végrehajtásának nehézségi fokát számos, a megtévesztővel, a közösségi média alkalmazásaival és szolgáltatásaival, a megtévesztő cselekedettel és a lehetséges áldozattal összefüggő tényező határozza meg. A magasabb nehézségi szint értelemszerűen elriasztja a potenciális elkövetőket, míg a nehézség alacsonyabb foka akár lehetőséget teremthet mások megtévesztésére is.

A megtévesztő

Számos, a megtévesztőhöz társított tényező szabja meg a nehézségi szintet, beleértve az elvárásait, a céljait, a motivációit, a célszemélyhez fűződő kapcsolatait és az esetleges áldozat gyanakvásának fokát (Buller & Burgoon 1996).

Az elvárások olyan alkotóelemet jelentenek, amely a siker valószínűségét határozza meg: az összetettebb üzenetek nagyobb valószínűséggel érik el céljukat (Madshusudan 2003). A cél és a motiváció szintén a megtévesztés nehézségi fokáról dönt. A cél tágabb és hosszú távú érvénnyel bír, ezzel szemben a motiváció bizonyos rövid távú célkitűzésekből tevődik össze. Egy David Buller és Judee Burgoon (1996) által kifejlesztett motiváció-taxonómia értelmében a megtévesztésnek három motivátora lehet:

1. *instrumentális*, amely során célirányos megtévesztés állapítható meg (például hazudni az önéletrajzban annak érdekében, hogy valaki több állásajánlatot kapjon);
2. *relációs* (más néven társadalmitőke-vonatkozású), amely a társadalmi kapcsolatok ápolását célozza (ez a közösségi oldalakon tipikus, lásd Squicciarini & Griffin 2012); és
3. az online profil jó hírnevének megvédése a káros eseményektől.

Az említett motivációs tényezők mindegyike meghatározza a félrevezetés költségét (a.m. a megtévesztés nehézségi fokát, tulajdonképpen a befektetett energiát és időt). Például a személyazonosságának meghamisításában érdekelt megtévesztőnek nagyobb erőfeszítéseket kell tennie a siker érdekében a mindennapi életben (offline) a nehezen hamisítható jelek jelenléte miatt, mint a világhálón, ahol számos személyazonosság alapú „nyom" (nem, kor stb.) mutatkozhat egyezményes jelként (például az előbbiek megjeleníthetők egy adott személy adatlapján hitelesítés nélkül). A megtévesztés nehézségét meghatározza a félrevezetésben érdekelt személynek a célszemélyhez való viszonyulása is.

Véleményünk szerint a fenti motivátoroktól és a megtévesztés kiszemeltjeitől függ az, hogy a családi viszony a célszeméllyel, illetve a szoros kapcsolat annak közeli szociális hálózatával megkönnyíti-e a bizalomszerzést és csökkenti-e a megtévesztés nehézségét, amint azt Michail Tsikerdekis és Sherali Zeadally (2014) állítja. Ha ugyanis a fentiek között szereplő 2. és 3. esetekről van szó, tehát valaki új arculatot épít, akkor az őt közelebbről ismerők előtt éppenséggel nehezebb magát hitelesítenie is.

Sok felhasználó feltételezi azt, hogy a technológia nagyobb biztonsággal jár, és nyugodtabban bíznak meg másokban (Castelfranchi 2001). Továbbá annak a bizalomnak a szintje, amelyet az egyének a megtévesztőbe vetnek, csökkenti gyanakvásuk fokát, növelve annak esélyét, hogy félrevezetés áldozatai lesznek.

Az erkölcsi költség megnehezíti a megtévesztést (Squicciarini & Griffin 2012). Az erkölcsnek erősen befolyásoló hatása lehet arra nézve, hogy a megtévesztők mit minősítenek erkölcstelennek az információ visszatartása vagy akár a hazugság terén. A való világban az interakció azonnalisága nagyban megnehezítheti egyesek számára a megtévesztést. Ezzel szemben világhálós környezetben a távolság és az anonimitás (Suler 2004) hozzájárul a gátlások csökkenéséhez vagy megszűnéséhez, csökkentve a félrevezetés morális költségeit a megtévesztő számára.

A közösségi média megköveteli tőlünk, hogy kibővítsük a látómezőnket arra, hogy miként történik a vevő és az adó közötti kölcsönhatások észlelése a megtévesztés során. A személyközi megtévesztés elmélete (Interpesronal Deception Theory – IDT) kimondja, hogy a vevő és az adó közötti kölcsönhatás valójában ismétlődő tapogatózások játéka, amelynek célja a megtévesztés sikere (Buller & Burgoon, 1993).

Judith S. Donath (1999) rámutatott, hogy a megtévesztés sikere annak egy adott világhálós közösségben való előfordulási valószínűségétől is függ. A precedensek értelemszerűen a gyanakvás magasabb fokához, egyszersmind kudarcba fulladt félrevezetési kísérletekhez, majd az adott online közösségen belül a megtévesztések megtorpanásához, megszűnéséhez vezetnek. A közösségi médiában a mindennapi világból ismert biztosítási mechanizmusok sokkalta nehezebben lépnek életbe, következésképp a tettenérés és a szankciók esélye is kisebb vagy kisebbnek tűnik, vagyis a megtévesztés költsége alacsonyabb.

Az úgynevezett információgazdagság szintén olyan tényező, amely meghatározza a megtévesztés nehézségét – Holtjona Galanxhi és Fiona Fui-Hoon Nah (2007) a „kibertérben" zajló megtévesztésekről szóló tanulmánya megállapítja, hogy a félrevezetőkre nagyobb stressz nehezedett akkor, ha szövegesen kommunikáltak, mint amikor azt képmással ellátott „csevegés" *(chat)* keretében tették.

Az időkorlát és a megtéveszteni kívánt személyek száma a megtévesztés sikerét szintén meghatározó tényező. A közösségi médiára jellemző aszinkron kommunikációs keretek miatt egyaránt fontos a rendelkezésre álló idő, valamint maga a tény, hogy több embert nehezebb megtéveszteni.

Megtévesztési technikák

A szakirodalom (például Nunamaker 2004) számos, a közösségi média környezetében gyakorolt megtévesztő technikáról számol be. Ilyen egyebek között a blöff, a mimikri (egy weboldal utánzása), a hamisítás (egy hamis weblap készítése), a kegyes hazugság, a kitérés, a túlzás, a weboldalak átirányítása és az eltitkolás (információk elrejtése az adatlapról).

Therani Madhusudan (2003) kommunikációs modellje alapján osztályozhatók a megtévesztési technikák és értékelhető azok hatékonysága. A modell egy adóból (S), tartalomból vagy üzenetből (I), és abból a csatornából (C) áll, amelyen a kommunikáció végbemegy. Ha a vevő (vagy fogadó, a továbbiakban felváltva használjuk a két kifejezést) által várt SIC-háromszög eltér a fogadott háromszög összetételétől, megtévesztésről beszélünk, amelynek hátterében az S, I, C elemeknek vagy azok kombinációjának manipulációja áll.

Tsikerdekis és Zeadally (2014) vizsgálódásai megállapítják, hogy az adó (más szóval a megtévesztő, S) személyazonosságának információira vonatkozó megtévesztés kis nehézségekbe ütközik, sikerességi esélyei pedig nagyok a blogok, a mikrobloggoló felületek, a közösségi híroldalak, a közösségi oldalak és a virtuális világok esetében. A tartalom-manipuláció mind a nyolc általuk vizsgált közösségi médiatípus esetében könnyűnek bizonyult, és az együttműködési projektek és a virtuális játékvilágok kivételével nagy megtévesztési sikereket hozott. A csatorna manipulációját pedig a közösségi oldalak és a virtuális (játék)világok adta keretek között jellemzi a nehézségek alacsony foka és a megtévesztési esélyek sikere.

A *tartalommanipuláció* a mások megtévesztésére feltehetőleg a leggyakrabban alkalmazott módszer. Ez a közösségi média adta kereteken belül az információk hamisításával történik. A blogok, az online multimédiás tartalmakat megosztó közösségek, a közösségi híroldalak, a mirkobloggoló felületek kimondottan fogékonyak a félrevezetés e módjára. A technológia elképesztő mértékben teszi lehetővé a multimédiafájlok manipulálását. A fényképek torzítása az egyik hatékony válfaja ennek a jelenségnek, amelynek eredményeként például egy felhasználó ismerősei körében az a képzet keletkezhet egyes módosított és a közösségi médiára feltett képek láttán, hogy ismerősük bejárta az egész világot. Ez a stratégia segíthet a megtévesztőknek társadalmi státusuk emelésében, valamint abban, hogy áldozatuk bizalmába férkőzzenek annak érdekében, hogy információkat szerezzenek.

Különösen nyilvánvaló mindez a Tinder nevű online társkereső alkalmazás tükrében, amelynek népszerűsége Liraz Margalit (2014) szerint az emberi evolúciós mechanizmushoz való illeszkedési képességében gyökerezik, vagyis az emberi fajnak a kevés rendelkezésre álló információ alapján tett gyors ítélkezéshez szükséges döntéshozatali apparátusa és ennek túlélést biztosító egyedfejlődési hagyományai mentén kifejlődött, örökletes és veleszületett pszichológiai architektúrájából/felszereltségéből következik.

A Tinder esetében a felhasználók korlátozott információk – tehát a keresztnév, a kor, a lakóhely, valamint képek – közzétételét követően kölcsönös, mindenekelőtt fizikai vonzalmon alapuló tetszésnyilvánítás eredményeként tehetnek szert további információkra. A megosztott tartalmak és képek magától értetődően lehetnek manipuláltak, egy elérni

kívánt, előnyös – akár teljesen hamis – arculat felépítésének szolgálatában. A képaláírásokból fakadó, identitásigénnyel fellépő, szimbolikus állítások és az olyan viselkedésnyomok, mint például a közelképek megosztásai által sugallt magabiztosság egyaránt azt hivatottak közvetíteni, hogy szerzőik milyennek szeretnének látszani. A felhasználóban pedig a lakhely és a kor racionális, illetve a küllem és a viszonzott érdeklődés emocionális tényezői nyomán öntudatlanul az a hiedelem ébredhet, hogy immár minden szükséges információval rendelkezik ahhoz, hogy potenciális, rövid vagy hosszú távú társáról tett első, valójában automatikus, irracionális és felületes benyomása megalapozott legyen (Margalit 2014). Az identitást meghatározó információk manipulációjáról a továbbiakban lesz még szó.

A képeken és a videókon felül a szövegalapú tartalom manipulációjának könnyedsége révén is minimalizálható a megtévesztésbe fektetett költség, és növelhető a siker valószínűsége. Ennek hátterében számos tényezőt találunk: ilyen az alacsony információs tudatosság a vevők/fogadók körében (a. m. a tartalom kritikus kiértékelése), és ilyenek az ellenőrizhetőség és az elszámoltathatóság hiányzó elvárásai. A profil kezelését a felhasználók számára elérhetővé tevő közösségi médiatípusok, – mint például a közösségi oldalak és a virtuális világok – szintén fogékonyak a tartalmi megtévesztésre, különösen azokban az esetekben, amikor új kapcsolatok kezdeményezésének népszerűsítéséről van szó, és a magánszféra védelme és a mások megtévesztése közötti határvonalak eleve elmosódhatnak. Az írás érzelmi aspektusaiban jártas megtévesztő nagy előnnyel rendelkezik az ilyen jellegű közösségi médiatípusok használata során.

Ezzel szemben a Wikipédiához hasonló együttműködési projektek kevésbé vannak kitéve a tartalom manipulációjának. Bár a megtévesztés kevésbé tűnik nehézkesnek, a siker esélye (legalábbis hosszú távon) szintén alacsony. Ez azért van, mert a közösségi média e köreihez sorolható szoftverek modelljei, amelyek által sokan kommunikálnak sokakkal, lehetővé teszik a tartalom több személy általi felülvizsgálatát. A tartalommanipuláció jelenlétére engednek következtetni a Wikipédián a mások megtévesztése érdekében az egyes bejegyzéseket manipuláló „vandálok" mellett a velük való harcot felvállaló személyek is (Solorio et al. 2013). Továbbá biztosítási mechanizmusok – mint a tartalom érvényességének követelménye (a.m. a tartalomnak a forráshoz való visszavezetése) – vannak beépítve a rendszerbe annak biztosítása érdekében, hogy a megtévesztés láthatóbbá, illetve elkerülhetőbbé váljon. További példát jelentenek a tartalommanipulációra az ilyen jellegű közösségi médiatípusok esetében a sok felhasználó által kezelt nyílt forráskódú szoftverek, amelyek esetében jóval nehezebb a rosszindulatú tartalom megosztása és a megtévesztés sikere, hiszen számos egyén értékeli a kódot, mielőtt az megjelenik. A virtuális játékvilágok terén szintén kisebbek a megtévesztés sikerének esélyei az olyan erősen narratív elemek miatt, mint azok a szerepek, amelyek a résztvevőre konkrét lépéseket és cselekménysorozatot rónak.

A megtévesztés történhet az adó (S) identitásinformációinak manipulálásával is. Ennek gyakran előforduló válfaja a megszemélyesítés, amely a személyazonosság-lopás kategóriájába esik (Wang et al. 2006). Ebben az esetben a megtévesztő másnak adva ki magát szerez információkat (például személyes adatokat: lakcímet, születési dátumot vagy telefonszámot) a társaitól. Mivel nincs lehetőség hitelesíteni az adó személyazonosságát és motivációit, a megtévesztés sikerességének esélyei kedvezőek. A közösségi média, amelyet az önképviselet és az önleleplezés magas foka jellemez, lehetővé teszi, hogy az adó kilétével összefüggő megtévesztés alacsony költségekkel történjen. A blogok és a mikrobloggoló felületek teret engednek az identitások ellopásának, hiszen esetükben nincsenek meg az új felhasználókat és a hozzájuk társuló neveket ellenőrző és azonosító kontrollmechanizmusok. Ugyanakkor az okozott kár is nagy valószínűséggel kisebb mértékű, és a hosszú távú siker sincs biztosítva. A személyazonosság tulajdonosaiban tudatosodhatnak a történtek, és a kárvallott személy ismerősei felismerhetik a személyazonosságtól idegen viselkedésmintákat. A közösségi oldalakon és a virtuális világok adta keretek között a megtévesztés költsége emelkedik, mivel a megtévesztő személy megnyilvánulásainak illeszkedniük kell az általa megszemélyesített identitáshoz tartozó viselkedésmintákhoz, és kognitívan meg kell felelniük azoknak. Ugyanakkor a haszon sokkal nagyobbnak tűnik a közösségi média kontextusában, hiszen egy egyén társadalmi hálózatához való hozzáférés megnöveli a visszaélés esélyeit. Nap mint nap számos példát látunk arra, hogy a Facebook-felhasználók felhívják ismerőseik figyelmét arra, hogy a „tőlük" származó információkat ne tulajdonítsák nekik, hiszen profiljukat feltörték, ami nemcsak a jelenség elterjedtségét, hanem a vele összefüggő aggodalmakat is tükrözi. Ezekben az esetekben azonban a megtévesztés célpontjai nem is feltétlenül azok a személyek, akiknek a személyazonosságát ellopták, hanem az ő ismerőseik, akik közül ráadásul a felhasználóprofillal nem rendelkező személyek a forrásokat ellenőrző kontrollmechanizmusok híján talán még inkább ki vannak téve a megtévesztésnek, mint azok, akik regisztráltak (Tsikerdekis & Zeadally 2014). Feltételezéseim szerint – bár empíria ezt egyelőre nem támasztja alá – az adóra vonatkozó

információk manipulációja felmerül a vallásos attributumok elrejtését vallásjogilag legitimizáló *taqiyya* doktrínájával összefüggésben, *par excellence* a világhálón folyó hittérítő tevékenységek (Iványi 2014a) szövegkörnyezetében is.

Az önmegjelenítés és az önleleplezés alacsony fokával járó együttműködési projektek vagy virtuális világok rendeltetésükből fakadóan értelemszerűen védettebbek az ilyen jellegű károkozásokkal szemben. Ezek, valamint az online multimédiás tartalmakat megosztó közösségek és a virtuális játékvilágok erőteljesen feladatalapúak. A megszemélyesített identitás társadalmi hálózatához hozzáférni kívánó személy útjába ez komoly akadályokat gördíthet, hiszen a feladatoknak megfelelő szerepek hitelesnek tűnő átvétele magas költséggel jár, a siker sincs szavatolva, érvénye pedig eleve rövid távra korlátozódik.

A tartalommanipuláció és az adó személyéhez köthető megtévesztés közötti szintként fogható fel az identitáshoz társuló információk manipulációja. Az ilyen akciók az identitás eltitkolásaként vagy meghamisításaként kategorizálhatók, amelyek keretében az eredeti identitásra vonatkozó információkat elrejtik és/vagy megváltoztatják, illetve új identitás épül (Wang et al. 2006). Előfordul, hogy valaki megkísérli elrejteni felhasználói profiljának egyes információit annak érdekében, hogy másokat megtévesszen, másnak vagy másként mutatkozzon meg, mint aki, vagy egyszerűen csak új arculatot épít – ez természetesen áttételesen a megosztásokat is érinti, bizonyos *customize*-funkciók útján. Mindez a legártatlanabb dolgoktól, mint például a közvetlen családtagok elől a felhasználót „rossz" színben feltüntető, mulatós képek elrejtésétől a nagy nyilvánosság előtt a valóságos politikai napirendek leplezett képmutatásán át a rejtett „zoknibábok" képében jelentkező titkosszolgálati megfigyelésekig terjed (Iványi 2014a, 2014b). A kommunikációs csatornára vonatkozó (C) megtévesztéssel összefüggésben Tsikerdekis és Zeadally (2014) megállapítja, hogy amíg a testbeszédhez hasonló nem verbális kommunikáció vagy bizonyos beszédminták felfedhetik a megtévesztőket, addig a közösségi médiában ez leküzdhető a nemkívánatos fázismodulációkkal (úgynevezett remegés, dzsitter) és a videókba, hanganyagokba tudatosan beékelt késleltetésekkel. A „vonal" másik végén az áldozat ugyanis nehezen tudja megkülönböztetni az akadozó/megbízhatatlan/lassú stb. összeköttetést a megtévesztés cselekedetének „finom részeitől".

A „keresztezett" megtévesztési technikák bevonják a korábban bemutatott SIC-modell több elemét, és növelhetik a megtévesztés hatékonyságát. Therani Madhusudan (2003) megállapítja, hogy az S, az I és a C közötti viszonyok egységes képet tárnak a vevő elé. Miként a mértanban, a háromszög egyik elemének módosulása inkonzisztens viszonyt teremt (például az S és az I között).

Számos olyan hibridtechnikáról tud a szakirodalom, amellyel mind a tartalmat, mind az adó információit manipulálják, beleértve egyebek között az identitáshamisítást, az emailes csalást és az adathalászatot (a tunéziai kormányzat bizalmas adatok megszerzésére törekvő adathalászatot folytatott [angolul: *to phish*], Facebook- és Gmail-jelszavakat csalva ki a felhasználóktól, lásd Iványi 2014b). Ezek nagyon hatékonyak lehetnek például a felhasználói identitásokat előtérbe toló és az egy-az-egyhez, illetve az egy-a-sokhoz kommunikációt megvalósító közösségi oldalak, virtuális világok, mikrobloggoló felületek és blogok esetében. Tsikerdekis és Zeadally (2014) példákkal illusztrálja azt, hogy egy-egy ilyen megtévesztésnek akár tragikus következményei is lehetnek. A hamis üzleteket képviselő weboldalak, amelyek egyszerre manipulálják az adó információit és a tartalmat, a felhasználó által kifejlesztett alkalmazásoknak és úgynevezett *widget*eknek (kisalkalmazások vagy minialkalmazások) a közösségi média szolgáltatásaiban való fokozatos elterjedése révén kapcsolódnak ide. A felhasználók a rosszindulatú szoftvereket felismerő felülvizsgálati mechanizmusok ellenére is sebezhetőek maradnak.

A megtévesztés különféle, online jelentkező, áttekintett eseteinek (a feladó személyére vonatkozó információk vagy a tartalom manipulációja, hibridtechnikák) tükrében e tanulmány konklúziója kettős. Egyfelől az, hogy a félrevezetés és annak sikere egyaránt a természetben gyökerezik, ezáltal a mindennapok része. Másfelől az, hogy a felállított adó–tartalom–csatorna-modellben leírható viszonyok szűrőmechanizmusai híján azok a nem verbális jelzések, amelyek adott esetben segíthetnének felfedni a vevő előtt a megtévesztésre irányuló motívumokat és az abban érdekelt személyek kilétét, a háttérben maradnak.

Irodalom

Bereczkei Tamás (2003): *Evolúciós pszichológia.* Budapest: Osiris Kiadó.

Brenner, Joanna & Aaron Smith (2013): 72% of Online Adults are Social Networking Site Users. *Pew Research Center,* augusztus 5. http://pewinternet.org/Reports/2013/social-networking-sites.aspx (letöltés: 2015. február 13.).

Buller, David & Judee Burgoon (1996): Interpersonal Deception Theory. *Commun Theory*, vol. 6, no. 3, pp. 203–242.

Burgoon, Judee & Mark Adkins & Matthew L. Jensen (2005): An Approach for Intent Identification by Building on Deception Detection. Syst Sci 2005 HICSS '05 Proc 38th Annu Hawaii Int Conf.

Czuczor Gergely & Fogarasi János (1865): *A magyar nyelv szótára.* Budapest: MTA.

Dai, Chenyun & Rao Fang-Yu & Traian Marius Truta & Elisa Bertino (2012): *Privacy-preserving assessment of social network data trustworthiness.* CERIAS Tech Report 2012-08 Privacy-Preserving Assessment of Social Network Data Trustworthiness. Augusztus. https://www.cerias.purdue.edu/assets/pdf/bibtex_archive/2012-08.pdf (utolsó letöltés: 2015. február 13.).

Donath, Judith S. (1999): Identity and deception in the virtual community. In: Mark Smith & Peter Kollock (eds.): *Communities in Cyberspace.* Routledge.

Dosztojevszkij, Fjodor M. (1975): *A Karamazov testvérek.* Budapest: Európa.

Ekman, Paul (2010): *Beszédes hazugságok. A megtévesztés árulkodó jelei a politikában, az üzletben és a házasságban*. Budapest: Kelly.

Előry Vilma, szerk. (2010): *Magyar Értelmező Kéziszótár Diákoknak.* Budapest: Tinta.

Iványi Márton (2014a): „Kiber-szubkultúrák": internet és radikalizmus. *Információs Társadalom*, 2. sz., 45–65. o.

Iványi Márton (2014b): Közösségi média: a nyilvánosság elektronikus agorája vagy posztmodern panoptikum? Hatalmi válaszok a közösségi média kihívásaira. *Médiakutató, nyár,* 119–138. o.

Kaplan, Andreas & Michael Haenlein (2010): Users of the world, unite! The challenges and opportunities of Social Media. *Business Horizons,* vol. 53, no. 1, pp. 59–68.

Madhusudan, Therani (2003): *On a text-processing approach to facilitating autonomous deception detection.* 2003 Proceedings of the 36th Annual Hawaii International Conference on System Sciences.

Margalit, Liraz (2014): Tinder and evolutionary psychology. Tech Crunch. http://techcrunch.com/2014/09/27/tinder-and-evolutionary-psychology/ (letöltés: 2015. február 9.).

Nazemroaya, Mahdi D. (2014): From energy war to currency war. *Global Research.* December 26. http://www.globalresearch.ca/from-energy-war-to-currency-war-americas-attack-on-the-russian-ruble/5421554 (letöltés: 2015. Február 15.).

Nunamaker Jr. Jay F. (2004): *Detection of deception: collaboration systems and technology.* Syst Sci 2004 Proc 37th Annu Hawaii Int Conf.

Pete, Krisztián: Hazugság. In: *Kommunikációtudományi Nyitott Enciklopédia.* http://ktnye.communicatio.hu/index.php?title=Hazugság (letöltés: 2015. február 9.).

Shen, Xuemin (2013): Security and privacy in mobile social network [Editor's Note]. IEEE Netw.

Solorio, Thamar & Ragib Hasan & Mainul Mizan (2013): A Case Study of Sockpuppet Detection in Wikipedia. In: Atefeh Farzindar & Michael Gamon & Meenakhsi Nagarajan & Diana Inkpen & Cristian Danescu-Niculescu-Mizil (eds.): *Proceedings of the Workshop on Language Analysis in Social Media.* Stroudsburg, PA: The Association for Computational Linguistics.

Squicciarini, Anna & Christopher Griffin (2012): *An Informed Model of Personal Information Release in Social Networking Sites.* In: Privacy, Security, Risk and Trust (PASSAT), 2012 International Conference on and 2012 International Conference on Social Computing (SocialCom).

Suler, John (2004): The Online Disinhibition Effect. *Cyber CyberPsychology & Behavior*, vol. 7, no. 3, pp. 321–326.

Tsikerdekis, Michail és Sherali Zeadally (2014): Online Deception in Social Media. *UKnowledge*. Szeptember. http://uknowledge.uky.edu/cgi/viewcontent.cgi?article=1013&context=slis_facpub (letöltés: 2015. február 13.).

Szun-ce (1963): *A hadviselés törvényei.* Budapest: Zrínyi.

Wang, Alan G. & Hsinchun Chen & Jennifer J. Xu & Homa Atabakhsh (2006): Automatically detecting criminal identity deception: an adaptive detection algorithm. Syst Man Cybern Part A Syst Humans, IEEE Trans. 2006, 36(5): 988–999.

Zahavi A. (1993): The Fallacy of Conventional Signalling. *Philosophical Transactions of the Royal Society of London. Series B, Biological Sciences*, vol. 340, no. 1292, pp. 227–30.

Iványi Márton arab filológus, közösségi médiakutató. Jelenleg PhD-tanulmányokat folytat a Corvinus Egyetem Társadalmi Kommunikáció Doktori Iskolájában. Főbb érdeklődési területei: a közösségi médiának az arab világ társadalmi mozgalmaiban játszott feltételezett szerepe, valamint az online közösségi hálózatok és a radikalizmus viszonyrendszere. Legutóbi írása a *Médiakutató*ban: „Közösségi média: a nyilvánosság elektronikus agorája vagy posztmodern panoptikum? Hatalmi válaszok a közösségi média kihívásaira" (2014. nyár).