Alapítva: 2001

INFORMÁCIÓS TÁRSADALOM

SZAKTUDOMÁNYOS FOLYÓIRAT

Kiss Attila – Krasznay Csaba: A felhasználói viselkedéselemzés kiberbiztonsági előnyei és adatvédelmi kihívásai

Hivatkozás/reference:

Kiss Attila és Krasznay Csaba, „A felhasználói viselkedéselemzés kiberbiztonsági előnyei és adatvédelmi kihívásai", Információs Társadalom, XVII. évf. (2017) 1. szám, 55-71. old.
http://dx.doi.org/10.22503/inftars.XVII.2017.1.4

Az elmúlt években a kiberbiztonság védelmi oldalán állók olyan lemaradásba kerültek a támadó oldallal szemben, amit soha korábban nem tapasztalhattunk. A távolság csökkentésére évről évre újabb megoldások kerülnek kidolgozásra, de jelenleg az egyik legkomolyabb „csodafegyvernek" a felhasználói viselkedéselemzést tartják. Felvetődik azonban a kérdés, hogy hogyan lehet a felhasználók magánszférájának, adatainak védelmét is biztosítani úgy, hogy a technológia teljes egészében a megfigyelésen alapul? Tanulmányunkban bemutatjuk a kiberbiztonság aktuális problémáit, az ezekre adott Big Data alapú lehetséges megoldásokat, valamint áttekintjük az adatvédelemmel kapcsolatos legfontosabb jelenlegi és az EU Általános Adatvédelmi Rendelete által 2018 májusától előírt jogi követelményeket.
Kulcsszavak: kiberbiztonság, adatvédelem, viselkedéselemzés, profilozás, Általános Adatvédelmi Rendelet

Cybersecurity Advantages and Privacy Challenges of User Behaviour Analytics

In recent decades those responsible for the defence of IT systems and infrastructure have significantly failed to keep up with those attacking them. New technologies appear from time to time in order to reduce this gap. According to our current knowledge, user behaviour analytics and/or entity behaviour analytics could mean light at the end of the tunnel. These tools, however, raise the question of how to ensure privacy and protect the personal data of users when technology is completely based only the constant surveillance of their digital world. This paper presents some of the recent IT security challenges together with possible solutions based on Big Data methods, then summarizes the key principles of data protection in light of the forthcoming General Data Protection Regulation of the EU in order to find a legal and ethically correct application of these IT security tools.
Keywords: cyber security, data protection, behavioural analytics, profiling, GDPR

Kiss Attila – Krasznay Csaba

A felhasználói viselkedéselemzés kiberbiztonsági előnyei és adatvédelmi kihívásai

Bevezetés

Azok számára, akik évek, évtizedek óta az információbiztonság területén dolgoznak, nem meglepő, hogy egyre több és egyre komplexebb támadás indul az információs infrastruktúrák ellen. Azzal azonban, hogy a média is egyre többet foglalkozik a kibertámadásokkal, illetve hogy a mindennapi ember is a saját bőrén érezheti ezek hatását, például a zsarolóvírusok jelentette közvetlen károk útján, kezd folyamatosan a közbeszéd részévé válni ez a fenyegetés. A kiberbiztonság objektív mutatói mellett tehát a szubjektív percepció is romlik, így a védelemmel foglalkozó szakértőknek olyan megoldásokat kell keresni, melylyel érdemben lehet javítani a helyzeten.

Mivel a biztonsági problémák okaként első helyen a felhasználók ismerethiányát szokták feltüntetni, napjainkban fokozottan jelenik meg a biztonságtudatossági oktatások fontossága. Ez azonban nem elégséges. A szofisztikált támadások során a tapasztalatok szerint a támadók biztosan megtalálják azokat a felhasználókat, akiknek a hibáit kihasználva be lehet jutni egy rendszerbe. Ezért a megoldásszállítók között folyamatos a versenyfutás a kiberbiztonság „Szent Gráljának" a megtalálásában, melynek segítségével a támadási kísérletek még korai fázisban észlelhetők és megállíthatók. Ilyen csodafegyver azonban valószínűleg nincsen. A létező technológiák jó összehangolása és a stratégiai gondolkodás vezethet oda, hogy a számítógépes rendszerekre leselkedő veszélyeket elfogadható szintre lehessen csökkenteni.

Ez persze nem jelenti azt, hogy ne lennének olyan innovatív megoldások, amelyek érdemben képesek javítani a kiberbiztonság állapotán. Az egyik ilyen megoldás a felhasználói viselkedés elemzése. Az informatikai erőforrások robbanásszerű fejlődése lehetővé tette, hogy a nagy mennyiségű digitális adatból, amelyet egy felhasználó a munkája során generál, létre lehessen hozni egy olyan profilt, amely a felhasználóra jellemző, „szokásos" tevékenységet mutatja be. Ezt használják ki az elektronikus kereskedelem során, például a közösségi oldalakon látható célzott, személyre szabott hirdetések a felhasználói profil alapján kerülnek megjelenítésre. Ha azonban ismert a „szokásos", akkor ismert a „szokatlan" tevékenység is. Ez ad lehetőséget a védelmi megoldások tervezésére, építve arra, hogy ha egy felhasználót sikeresen támadnak, majd a hozzáférési jogosultságaival visszaélve bejutnak a rendszerbe, akkor a humán karakterisztikák megváltoznak, hiszen más ember, más szokásokkal fogja a rendszert használni. Ezt a változást pedig jó eséllyel detektálni tudja a rendszer.

A jó védelem azonban folyamatos megfigyeléssel jár, hiszen ez az alapja a hatékony felhasználói profil felépítésének. Ahol pedig megfigyelés van, ott fokozottan kell figyelni a személyes adatok kiemelt védelmére is, hiszen a begyűjtött adatok részletes információt nyújtanak még a felhasználó által végzett legapróbb tevékenységről is. Ezzel pedig el is érkeztünk a biztonság kontra személyes adatvédelem kérdéskörhöz, mely a Snowden-féle szivárogtatás óta kiemelt figyelmet kapott az egész világon. Érdemes tehát részletesebben is megismerni, mit nyerhet és milyen áron a társadalom a mesterséges intelligencia és a Big Data elemzés elterjedésével!

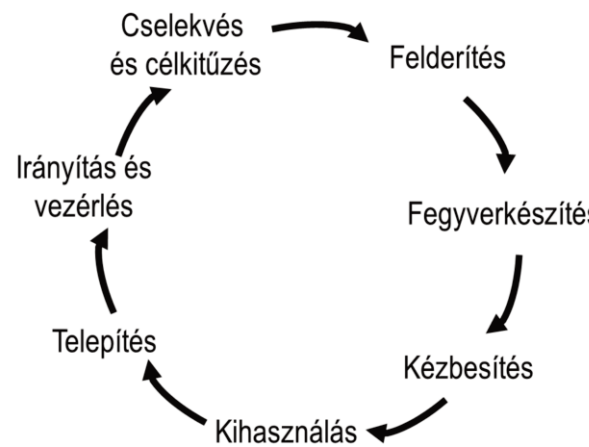
A kiberbiztonság aktuális kihívásai

Sokan, sokféleképpen próbálják megbecsülni, mekkora kárt okoz a globális gazdaság számára a kiberbűnözés. A Cybersecurity Ventures (2016) elemzése 3 billió dollárra teszi a jelenlegi károsszeget, mely véleménye szerint 2021-re akár 6 billió dollárra is felkúszhat, beleértve ebbe minden direkt és indirekt káreseményt, így a személyes adatok szivárgása okozta kárt, üzleti titkok nyilvánosságra kerülését, esetleg (kritikus) infrastruktúrák sérülését. A Ponemon Institute (2016) riportja szerint egy nagy szervezetnek évente átlagosan 4 millió dollár kárt okoznak a kibertámadások. Bár ezek a számadatok nem feltétlenül pontosak, még ha nagyságrendi tévedések is vannak bennük, mutatják, hogy mekkora gazdasági kárt okoz az informatikának való kitettség. Egyben mutatja azt is, hogy a kiberbűnözéssel foglalkozó csoportok bevétele is milliárd dollárokban mérhető, bár erre leginkább az egyes online identitások feketepiaci áraiból lehet következtetni. A Dell Secureworks (2016) gyűjtése szerint például egy „átlagos" üzleti felhasználói fiók ára a Darkweben 20 és 149 dollár között van, egy európai bankkártya adatait pedig 40 dollárért lehet megvásárolni. Ilyen digitális adatok pedig milliószámra állnak rendelkezésre az erre szakosodott bűnszervezeteknél.

Nehezen választható el a kiberbűnözéstől az államilag támogatott kiberkémkedés és a kiberhadviselés, hiszen ezek személyi és technológiai háttere gyakran összefolyik. Miután a NATO a 2016-os varsói csúcson hivatalosan is műveleti területté nyilvánította a kiberteret, nem csak a szervezetek egyéni védelmében, hanem a nemzetvédelemben is kritikussá vált az információbiztonság kiemelt kezelése – hivatalosan is (Minárik 2016). Nem véletlen, hogy napjaink politikai diskurzusában az egyik első kérdés, amit a megválasztott politikai vezető megkap, a kiberbiztonsággal kapcsolatos terveiről szól (Lee 2016).

Függetlenül attól, hogy mi a támadói motiváció, a végrehajtás eszköztára nagyon hasonló minden esetben. Hutchins és szerzőtársai (Hutchins et al. 2011) alapműnek számító cikkükben mutatták be a modern kibertámadások folyamatát és az elhárítás eszközeit. A folyamat az 1. ábrán látható. A jelen tanulmány szempontjából kulcsfontosságú Kézbesítés pontnál a következő megfogalmazás olvasható: „A fegyverként használható tartalmak három leginkább elterjedt célbajuttatási módszere a Lockheed Martin Computer Incident Response Team (LM-CIRT) 2004-2010 közötti megfigyelései alapján az e-mail csatolmányok, a weboldalak és a hordozható USB eszközök". Ez a megállapítás továbbra is igaz, egyben jelzi, hogy a támadó és a célpont közötti elsődleges kapcsolat egy, a szervezet infrastruktúrájához hozzáféréssel rendelkező személy. A védekezésben pedig éppen ezért kiemelt szerepe van az éber felhasználónak, aki képes a támadást észrevenni.

Pusztán a felhasználói éberségre azonban nem lehet építeni. A Nemzetközi Távközlési Unió adatai szerint 2016 végén a világ népességének 47%-a használja az internetet (ITU 2016). Egy nagyvállalatnál több tízezer ember rendelkezik valamilyen szintű hozzáféréssel az informatikai rendszerhez. Ebben a tömegben elég egy figyelmetlen vagy képzetlen felhasználó és a legfontosabbnak tartott védelmi vonal máris elesett. Nemeslaki és Sasvári (2014) a hazai biztonságtudatosság helyzetét vizsgálva is hasonló megállapításra jut, felmérésük alapján az üzleti és a közszférában dolgozók több mint harmada meg van győződve arról, hogy a számítógépük nem potenciális célpontja egy rosszindulatú támadásnak. Éppen ezért ma már minden szakembernek azzal kell számolnia, hogy a Kézbesítés sikeres lesz, így a későbbi fázisokban kell a megfogni a támadást.



1. ábra: Pusztítási lánc a kibertérben
(Hutchins et al. 2011)

A későbbi fázisokat elsősorban műszaki eszközökkel lehet kontroll alatt tartani. A hagyományos védelmi filozófia a megelőző (preventív) intézkedéseket részesíti előnyben, azaz olyan technológiák használatát, melyek nem engedik végrehajtódni a pusztítást kifejtő kódokat, illetve blokkolják a kompromittált erőforrásokhoz való távoli hozzáférést. Ezeknek a preventív megoldásoknak azonban hátránya, hogy elsősorban a korábbról már ismert támadási mintákat képesek kezelni, azaz a minta kis változtatásával a védelmi hatékonyság drasztikusan csökkenthető. Az elmúlt években emiatt a stratégiai gondolkodás változik, egyre jobban előtérbe kerülnek a felismerő (detektív) megoldások, melyek a több forrásból érkező információk alapján próbálják segíteni a támadások felismerését.

A klasszikus felismerő védelmi intézkedések közös tulajdonsága, hogy minél több forrásból érkező adat feldolgozásával segítik a döntéshozatalt, azaz annak eldöntését, hogy valójában kiberbiztonsági incidens történt-e. A két legrégebben használt technológia ezen a területen a behatolás-detektáló rendszer (Intrusion Detection System – IDS) és a rendszerek naplóadatait feldolgozó rendszer, melynek jelenleg bevett elnevezése biztonsági incidens- és eseménymenedzsment rendszer (Security Incident and Event Management – SIEM). A két rendszer között több a hasonlóság, mint a különbség. A fő eltérés az, hogy míg az IDS a hálózati forgalom elemzésére támaszkodik, a SIEM rendszerek a különféle naplóadatok közötti korrelációkból építkeznek. Ezen túlmenően főleg a hasonlóságokat érdemes vizsgálni!

A két technológiában közös, hogy hatalmas mennyiségű adatból tudnak építkezni, mely adatok strukturáltak ugyan, de az egyes források adatformátuma jellemzően különböző. A döntéstámogatást szabályalapon segítik, azaz a rendszerek által korábbról már ismert mintázatok alapján jelzik az esetleges behatolást. Hatalmas mennyiségű riasztást generálnak, így a nem megfelelően finomhangolt rendszer riasztásainak áttekintéséhez jelentős emberi erőforrás szükséges. Nagyon gyakoriak a hamis pozitív riasztások, melyek miatt a szabályrendszert folyamatosan finomítani kell. Eközben a valódi támadások, me-

lyek nem szerepelnek az ismert mintázatok között, könnyen rejtve maradhatnak.

Ezek a kihívások vezettek el ahhoz a felismeréshez, hogy mindkét technológiát érdemes olyan irányba fejleszteni, amely felhasználja a mesterséges intelligenciával kapcsolatos aktuális kutatásokat, hiszen alapvetően minden rendelkezésre áll a számítógéppel támogatott döntéshozatalhoz – a nagy mennyiségű adat és az igény arra, hogy ezekből minél hasznosabb információ álljon elő. A 2000-es évek közepén már számos kutató publikált az IDS-ek jövőjéről, például Abraham és szerzőtársai (2005) így fogalmazták meg a state-of-the-art helyzetet:

> „A behatolás-detektálásnak két típusa van: a nem szabályszerű használat és az anomália detektálása. A nem szabályszerű használat azonosításához a támadás azon jól definiált mintázatát használják, melynek segítségével ki lehet használni egy rendszer vagy alkalmazás sebezhetőségét. Ezek a mintázatok előre be vannak kódolva a rendszerbe és pontosan meg kell egyezniük a felhasználói tevékenységgel a behatolás detektálásához. Az anomália alapú behatolás-detektálás a normális felhasználás mintázatát használja a behatolás érzékeléséhez. A normális felhasználás mintázatát a rendszerek statisztikai értékeiből állítják elő. A felhasználó viselkedését ebben az esetben folyamatosan megfigyelik és bármilyen eltérést az összeállított normális viselkedésmintától behatolásként érzékelnek."

Elemzésük célja annak kimutatása volt, hogy mennyire hatékonyak az egyes gépi tanulási algoritmusok a kor lehetőségei mellett. Megállapították, hogy a mesterséges intelligencia jelentős segítséget nyújt a támadások észlelésében, de így fogalmazták meg a szükséges kompromisszumokat: „Az IDS által ellenőrizendő adathalmaz hatalmas, még egy kis hálózat esetében is. Az elemzés rendkívül nehéz még számítógépes támogatással is, mivel bizonyos elemzési módok nehézzé teszik a gyanús viselkedési mintázatok felfedezését. Az elemzési eredmények között komplex kapcsolatok vannak, melyeket a gyakorlatban emberi értelemmel lehetetlen felfedezni. Az IDS-ben ezért csökkenteni kell a feldolgozott adatok mennyiségét."

Hasonló kihívásokkal szembesültek a SIEM rendszerek üzemeltetői és a kor színvonala mellett hasonló irányban folytak a kutatások is. A matematikai és az informatikai háttér fejlődésével azonban folyamatosan jelentek meg azok a megoldások, amelyek lehetővé tették a nagy mennyiségű strukturált (és nem strukturált) adat hatékony elemzését, közel valós időben. 2010 környékén már a közösségi hálózatokat és a keresőmotorokat fejlesztő cégek elsődleges üzleti modelljévé vált a „normális" viselkedés, a felhasználók érdeklődési körének egyre pontosabb kiismerése. Csak idő kérdése volt, hogy mikor jelenik meg a kiberbiztonságban is ez a technológia, amely segíteni tud a „szokatlan" viselkedés azonosításában, ezzel megoldást kínálva arra, hogy túl lehessen lépni a hagyományos, szabályalapú megelőző és észlelő védelmi rendszerek adta határokon.

Felhasználói viselkedéselemzés a kiberbiztonságban

A bűncselekmények előrejelzése, ezzel pedig a biztonság növelése régóta foglalkoztatja az emberiséget. Elég csak Philip. K. Dick klasszikus novellájára, a Különvéleményre gondolni, mely már 1956-ban felvetette azt a kérdést, milyen kihívásokkal jár az, ha a „mes-

terséges" intelligencia segíti az emberiséget a bűnmegelőzésben, lényegében bizonyítékok nélkül ítélve bűnösnek a jövőbeni elkövetőt. Bár sokaknak eszébe jut ez az analógia a Big Data elemzés, a mesterséges intelligencia és a biztonság kapcsán, a társadalmi nyereség mégis olyan előnyösnek látszik, hogy az államok egyre jobban támaszkodnak ezekre a technológiákra, szélesebb körben kívánják azokat alkalmazni, akár az állampolgárok magánszférájának, információs önrendelkezési jogának korlátozása, szűkítése mellett is.

Természetesen számos olyan terület létezik, ahol közmegegyezés van az államok és az állampolgárok között abban, hogy a biztonság javítása érdekében a személyes adatok védelmét valamennyire háttérbe kell szorítani. Iverson (2015) kutatásában hat ilyen területet jelölt meg: a nemzetbiztonságot, a közbiztonságot, a tulajdon biztonságát (például kamerás megfigyeléssel), az információbiztonságot, a családok biztonságát (egészségügy) és a pénzügyi biztonságot.

A magánszféra védelméhez fűződő alapjog korlátozása ezeken a területeken jellemzően törvényi szinten került rögzítésre[1], de az információbiztonság és a hozzá kapcsolódó tulajdon biztonsága területén főleg a kialakult adatvédelmi joggyakorlat és a nemzeti adatvédelmi hatóságok, bíróságok jogértelmezése adhat csak iránymutatást. A rögzített jogok és kötelezettségek többnyire világosak, a Big Data és a mesterséges intelligencia azonban olyan értelmezési nehézségeket, kiskapukat hoztak a rendszerbe, melyek számos új kérdést vetnek fel a biztonság és az adatvédelem kapcsolatában.

Ezt legerőteljesebben Edward Snowden, a Booz Allen Hamilton cégen keresztül az amerikai National Security Agencynek (NSA) dolgozó elemző világot megrengető szivárogtatása támasztotta alá. Az NSA megfigyelési tevékenysége súlyosan sértette azokat az adatvédelmi elveket, melyeket az Európai Unióban természetesnek veszünk, de még a jóval megengedőbb, az információ szabadabb áramlását támogató amerikai jogrenddel is ellentétes volt a kialakított adatgyűjtési gyakorlat. Lyon (2014) összefoglaló cikkében mutatja be mindazt, amit a Snowden szivárogtatás által tudott meg a világ a Big Data felhasználásáról a nemzetvédelmi szektorban. Cikkének konklúziójaként két megállapítást tesz.

> „Egyrészt, milyen módon és milyen mértékben jelzi a Snowden-szivárogtatás azt, hogy a Big Data alkalmazása egyre fontosabb a megfigyelésben? A válasz egyértelműen az, hogy nagyon fontos. A legfontosabb Snowden-felfedések, különösen azok, amelyeknél a metaadatok kiemelt fontosságúak, függést mutatnak a Big Datától. A második kérdés az, hogy mennyire változtatják meg ezek a technikák a megfigyeléssel kapcsolatos politikát és gyakorlatot? Új trendek vannak, vagy a korábbiak kiterjesztéséről van szó? A bizonyítékok ismét arra utalnak, hogy a Big Data használata erősen torzítja a megfigyelést a technológiai

[1] Lásd például a tájékoztatáshoz fűződő jog korlátjaként az információs önrendelkezési jogról és az információszabadságról szóló 2011. évi CXII. törvény (a továbbiakban: Infotv.) 19.§-ban megjelenő területeket, ahol az érintett jogait törvény korlátozhatja: „az állam külső és belső biztonsága, így a honvédelem, a nemzetbiztonság, a bűncselekmények megelőzése vagy üldözése, a büntetés-végrehajtás biztonsága érdekében, továbbá állami vagy önkormányzati gazdasági vagy pénzügyi érdekből, az Európai Unió jelentős gazdasági vagy pénzügyi érdekéből, valamint a foglalkozások gyakorlásával összefüggő fegyelmi és etikai vétségek, a munkajogi és munkavédelmi kötelezettségszegések megelőzése és feltárása céljából – beleértve minden esetben az ellenőrzést és a felügyeletet is –, továbbá az érintett vagy mások jogainak védelme érdekében."

megoldástól való függés irányába (...) megnövelve a prediktív analitika fontosságát annak érdekében, hogy előre lehessen látni, meg lehessen jósolni bizonyos történéseket."

Ez a fajta függés a technológiától azonban nagyon veszélyes. Boyd és Crawford (2012) részletesen kifejti, mennyi kérdést vet fel a Big Data elemzés használata. Cikkükben hat olyan területet fogalmaznak mely, amelyeknek mindenkit aggodalommal kell eltölteniük a Big Data korlátlan használata esetén. Tanulmányunk szempontjából talán a legérdekesebb kritikai észrevétel az, hogy a kontextusból kiragadott Big Data eredmény elveszíti a jelentését, valamint az, hogy attól még, hogy valami hozzáférhető, még nem feltétlenül etikus a felhasználása. A biztonsági rendszerek sajátossága, hogy bár hihetetlen mennyiségű információt lehet belőlük kinyerni, kiemelt figyelmet kell fordítani arra, hogy a döntés meghozatalánál ezt az információhalmazt etikusan, a kontextus ismeretében használják fel.

Egy számítógép azt teszi, amit a programozója mond, így komoly hiba lenne egy program kimenetére bízni egy automatikus döntést. A Big Data és a mesterséges intelligencia azonban olyan lehetőség a biztonsági szakma kezében, amelyet egyértelműen használni kell. Olyan megoldásokat kell tehát fejleszteni, amelyek figyelembe veszik azokat az etikai elveket, amelyek egyébként az egyes európai és nemzeti adatvédelmi szabályokból is levezethetők.

A felhasználói viselkedéselemzés jogi szemszögből

Fel kell tennünk a kérdést ugyanakkor, hogy mennyiben jelenthetnek jogszerű megoldást a kibertér kihívásaira az itt bemutatott megoldások, illetve az azok továbbfejlesztésének eredményeképpen született – a viselkedést egyre több adatot felhasználva, még több szemszögből, hatékonyabban elemző és már előre is jelző – új rendszerek.

Általánosságban elmondható, hogy a viselkedésminta kialakítása, vagy az információs rendszer szokásos adatforgalmának meghatározása érdekében az érintett felhasználó számos adata rögzítésre kerül. Az elemző rendszerek figyelhetik a böngészési szokásait, elektronikus levelezését, a letöltött csatolmányainak tartalmát, a belső munkahelyi információs rendszer használatát, sőt a metaadatok mellett rögzíthetik akár az elektronikus kommunikáció tartalmát is.

Ha ezek az adatok később külön-külön, vagy akár kombinálva összefüggésbe hozhatóak maradnak az egyes felhasználókkal, vagy azokból következtetés vonható le az érintett természetes személyre, akkor – annak helytállóságától, etikai megítélésétől, jogszerűségétől, esetleges következményeitől függetlenül – személyes adatok kezeléséről beszélünk (Adatvédelmi Munkacsoport 2010 és Infotv. 3.§).

Gyakran hallani a profilozást folytató adatkezelőktől, hogy valójában nem kezelnek személyes adatot, hiszen csak a hálózathoz csatlakoztatott eszközöket figyelik, nem az azt használó magánszemélyt. Szintén gyakori érv, hogy a gyűjtött adatokat álnevesítik[2], illetve

[2] A közhiedelemmel ellentétben nem elegendő a természetes azonosító adatot egy számsorra cserélni, az álnevesítés adatvédelmi és adatbiztonsági követelményeit a 29. cikk szerinti Adatvédelmi Munkacsoport 05/2014. számú véleményében találjuk.

anonim módon gyűjtik, tehát ők nem kötelesek megfelelni adatvédelmi jogi követelményeknek. Ohm (2009) kutatási eredményei ugyanakkor azt mutatják, hogy az anonim adattárolás illúzió[3] az olyan adatgyűjtések esetében, ahol elegendően nagyszámú adat és idő áll rendelkezésre, így tipikusan a profilozás során is. Alexin (2014) bemutatja, hogy már három, első ránézésre az érintetthez szorosan nem kapcsolható azonosító (irányítószám, nem, születési dátum) összekapcsolásával is nagy valószínűséggel egyetlen személyt azonosíthatunk be. A viselkedéselemzést végző személy vagy szervezet (a továbbiakban: adatkezelő) tevékenysége pedig pont erre irányul – szeretné fokozatosan felismerni a felhasználó (jogi szóhasználatban: érintett) szokásait, gyakori hibáit, vagy érdeklődési körét, hogy aztán bizonyos esetekben egyre pontosabban tudja előre jelezni az érintett várható viselkedését egy adott élethelyzetben. A viselkedéselemzés – függetlenül attól, hogy a profilozás célja az információbiztonság fenntartása, a dolgozók teljesítményének (hasznosan töltött munkaidejének) monitorozása, vagy akár személyre szabott tartalmak, reklámok megjelenítése – veszélyt jelent az érintett alapvető emberi jogaira és szabadságaira (Nemzetközi Távközlési Adatvédelmi Munkacsoport 2013).

Számos nemzetközi dokumentum rögzíti az érintett magánélete tiszteletben tartásához fűződő jogát, beleértve kommunikációjának bizalmas jellegét és személyes adatai védelmét.[4] E jogoknak – bár esetenként korlátozottan – érvényesülniük kell a személyes adatok kezelésének valamennyi területén, beleértve a rendőrségi, igazságügyi, valamint a nemzetbiztonsági célú adatkezeléseket is.[5] Az Emberi Jogok Európai Bírósága kimondta emellett, hogy napjainkra a magán- és a szakmai élet kérdései nehezen különíthetők el egymástól, így a munkahelyi viselkedés és kommunikáció megfigyelése szükségszerűen beavatkozást jelent az érintettek magánéletébe is.[6] A levélküldemények felbontását és a telefonok lehallgatását vizsgáló döntéseken[7] túl a Bíróság kimondta azt is, hogy a munkahelyi e-mailek tartalma, sőt kommunikációjának metaadatai is az érintett védendő személyes adatai.[8]

Fontos kiemelnünk, hogy nem vonatkozik azonban adatvédelmi jogi előírás azokra az adatkezelésekre, amelyek kizárólag magáncélból történnek. Ennek tekinthető például, ha egy profilozást végző természetes személy pusztán a saját információs rendszere védelme érdekében vesz igénybe egy monitorozást végző terméket, és így készít viselkedésmintát saját magáról, amelyhez más, még az elemző szoftver gyártója sem férhet hozzá.

Ettől a nem túl gyakori esettől eltekintve azonban az Európai Unió valamennyi tagállamában szigorú jogszabályi követelmények kapcsolódnak az üzleti életben és a közszfé-

[3] *A deanonimizálás lehetőségeiről részletesen ír jelen lapszámunkban Gulyás Gábor György – a szerk.*

[4] A Liszaboni Szerződéssel 2009-ben elfogadott Európai Unió Alapjogi Chartájának 7. és 8. cikke tovább pontosította az Európa Tanács országai által 1950-ben elfogadott Emberi Jogok Európai Egyezményének 8. cikkében kifejtett alapjogot.

[5] Az EU adatvédelmi tárgyú jogszabályai 2018. májusig csak a nemzetközi adatáramlás kapcsán tartalmaznak kötelező előírásokat e területen, de az Infotv. hatálya és az Európa Tanács 108. egyezménye már most is kiterjed ezekre.

[6] Elsők között a Niemietz kontra Németország (13710/88) ügyben mondja ki az Európa Tanács 108. egyezménye kapcsán, de az ebben lefektetett elveket később az Európai Unió Bírósága is átveszi.

[7] Lásd például az Emberi Jogok Európai Bíróságának Halford v. Egyesült Királyság (1997) 20605/92. ügyében.

[8] Lásd bővebben az Emberi Jogok Európai Bíróságának Copland v. Egyesült Királyság (2007) 62617/00. ügye.

rában is a személyes adatok gyűjtéséhez, elemzéséhez, összefoglalóan kezeléséhez. Ezek azonban főleg az elveket rögzítik, ritka az egyes technológiákra vonatkozó speciális előírás, így a viselkedéselemzésen alapuló megoldások esetében is főleg az adatvédelmi hatóságok jogértelmezése, gyakorlata az irányadó.

Az alapelvek jelentősége

Az adatkezelés, így a profilozás is csak megfelelő korlátok között, jogszerű célhoz kötötten és megfelelő jogalap birtokában, az érintett jogait – kiemelten a tájékoztatáshoz (hozzáféréshez) fűződő jogát – tiszteletben tartva, valamint az adatok biztonságát garantálva válhat jogszerűvé.

Az adatminimalizálás és célhoz kötöttség elve alapján csak a jogszerű adatkezelési cél megvalósításához feltétlenül szükséges adatok gyűjthetőek, és csak olyanok, amelyek alkalmasak is annak eléréséhez. Az így gyűjtött adatokat ezt követően is csak az eredeti célhoz kötötten lehet felhasználni. Jogellenes például az információbiztonság, a rendszer védelme céljából gyűjtött adatok alapján meghatározni a dolgozó munkával töltött idejét, pártállását, vagy szabadidős érdeklődési körét. Szintén tilos az előre meghatározott cél nélküli, későbbi felhasználás érdekében történő úgynevezett „készletező adatgyűjtés".

A törvényes cél érdekében is csak akkor kezelhető személyes adat, ha megfelelő jogalappal történik. Meg kell különböztetnünk az érintett hozzájárulásán alapuló adatkezelést (Infotv. 5.§ (1) a)), törvény vagy – törvény felhatalmazása alapján, az abban meghatározott körben – helyi önkormányzat rendelete által előírt „kötelező" adatkezelést (Infotv. 5.§ (1) b)), illetve az érdekmérlegelésen alapuló eseteket (Infotv. 6.§).

A viselkedéselemzéshez közvetlenül kapcsolódó követelmény az adatminőség elvének való megfelelés is, amely előírja, hogy csak naprakész, pontos, és jogszerű forrásból származó adatok alapján vonjunk le következtetést a felhasználóról. Ide kapcsolódik az Európai Unió Bírósága által kifejtett[9], és az EU adatvédelmi reformjában is megjelenő „jog az elfelejtődéshez" (Right to be forgotten)[10] elve. Székely (2013) szerint e jog „érvényesíthetőségének előfeltétele, hogy az emberek egyáltalán tudatában legyenek annak, hogy ki, milyen célból, milyen adataikat kezeli – azaz gyűjti, elemzi és felhasználja – és azok törlését hol követelhetik. Ellenkező esetben hiába lesz jogunk ahhoz, hogy elfelejtsenek és töröljenek, ennek gyakorlati érvényesíthetőségétől egyre messzebb kerülünk." Az elfelejtődéshez való jog tehát úgy garantálható, ha az érintett tisztában van azzal, hogy milyen adatkezelés alanya (titkos megfigyelés csak bírói felügyelettel, törvény alapján végezhető), a cél megvalósulása érdekében pedig a lehető legkorábban tájékoztatni kell a profilozásról.

További előírásokat találhatunk még az adatkezelés időtartamára, az adatfeldolgozó igénybevételére és az adattovábbításra vonatkozóan is, valamint az adatkezeléseket be kell jelenteni az adatvédelmi hatóság, nálunk a Nemzeti Adatvédelmi és Információszabadság Hatóság (a továbbiakban: NAIH) által vezetett adatvédelmi nyilvántartásba.

[9] Lásd C-131/12. Google Spain v AEPD and Mario Costeja Gonzalez ügy.
[10] Más fordításban: Jog ahhoz, hogy elfelejtsenek.

A viselkedéselemzés jogszerű alkalmazási területei

A korábbiakban elemzett biztonsági kihívások miatt az új védelmi technológiák alkalmazása néhány területen a veszélyek ellenére is indokoltnak tűnik. Az állami szereplők oldaláról komoly nemzetgazdasági, bűnüldözési, nemzetbiztonsági, honvédelmi érdek fűződik a tömeges adatgyűjtésen alapuló detektív megoldások rendszeresítéséhez, míg a piaci szektor gazdasági megfontolások alapján – a munkavállalók okozta biztonsági kockázatok csökkentése, esetleg a teljesítményük mérése, javítása érdekében – vezetné be széles körben azokat. Kevés kritika éri az ügyfelek bankkártyás tranzakcióinak bankok általi monitorozását, amely lehetővé teszi a szokásostól eltérő helyen, vagy időpontban történő fizetések észlelését, az esetleges visszaélések megelőzését (Tamásné 2015). Nem szabad elfelejtkeznünk a jelenleg legszélesebb körben alkalmazott marketing célú profilozásról sem, amikor a közösségi oldalak és egyéb online üzleti szereplők a vásárlók szokásainak megismerésével kívánják javítani keresési eredményeiket – és ahhoz szorosan kapcsolódva eladási statisztikáikat.

Ezek a célok szintén visszavezethetőek az adatkezelők olyan alapjogi szinten is elismert jogaihoz, mint a vállalkozás szabadsága vagy a tulajdonhoz való jog.[11] Ezért a profilozást néhány területen tekinthetjük jogszerű célnak, azok szűk körben történő alkalmazására már most is lehetőséget (jogalapot) biztosít a magyar és az Uniós adatvédelmi jog is.

A tudományos diskurzus és az adatvédelmi hatóságok elsősorban a közvetlen üzletszerzés érdekében történő (reklám célú) viselkedéselemzés vizsgálatából indultak ki[12], és az EU 2018-tól alkalmazandó új adatvédelmi jogszabálycsomagja is különös hangsúlyt fektet a keresőoldalak és a közösségi oldalak komoly profitot eredményező profilozó tevékenységére. Ezekben az esetekben a felhasználó többnyire valamely szolgáltatás díjmentes igénybevételéhez kapcsolódva, annak szerződési feltételei között olvasható tájékoztatás birtokában, *hozzájárul* ahhoz, hogy róla adatokat gyűjtsenek. Bár ebből hátrányai származhatnak, de dönthet úgy, hogy nem regisztrál egy közösségi oldalra, vagy másik keresőoldalt vesz igénybe, esetleg letiltja az operációs rendszer naplózási funkcióját, vagy törli magát a levelezőrendszerből, ha nem kíván alanya lenni a viselkedéselemzésnek. Az elemzés során az adatkezelésnek végig meg kell felelnie a korábban bemutatott alapelveknek, igaz, a gyakorlat az mutatja, hogy ezek a súlyos adatvédelmi bírságok ellenére sem valósulnak meg a nagy nemzetközi vállalkozások esetében (lásd Google- és Facebook-perek szerte Európában).

A hatályos uniós jog, és a 2018-tól alkalmazandó szabályok alapján is a tagállamok szuverén joga marad, hogy *közérdeken alapuló célból jogszabályban* előírjanak egyes adatkezeléseket, így például lehetővé tegyék a viselkedéselemzést nemzetbiztonsági vagy honvédelmi érdekből néhány területen, vagy korlátozzák az érintett hozzáférési jogát a róla gyűjtött adatokhoz (például bűnüldözési érdekből). Hazánkban ágazati törvények lehetővé tehetik a viselkedéselemzést, amennyiben alkalmazásának feltételeit és korlátait megfelelően meghatározzák. Annak gyakorlati végrehajtása során azonban már figyelemmel kell

[11] Az Európai Unió Alapjogi Chartájának 15-17. cikkei is nevesítik ezeket.

[12] A tagállami adatvédelmi hatóságok egységes jogértelmezésük kialakítása céljából az EU adatvédelmi irányelvének 29. cikke szerinti Adatvédelmi Munkacsoportban (a továbbiakban: Adatvédelmi Munkacsoport) közös véleményt fogalmaztak meg a témában (2010 és 2011).

lennie az adatkezelőnek az adatvédelmi alapelvekre, csupán a jogalapjában tér el az érdekmérlegelésen, vagy az érintett hozzájárulásán alapuló adatgyűjtéstől.[13]

Noha a hatályos jogban nem találunk az információbiztonsági célból történő viselkedéselemzést előíró közvetlen jogszabályt, a jogalkotó is elismeri az információbiztonság jelentőségét, hiszen a személyes adatok védelme sem valósítható meg az adatbiztonsági elvárások (Infotv. 7.§) teljesülése nélkül. Az adatvédelmi incidens naplózásának előírásával (Infotv. 15.§) azt már nemcsak célként, hanem törvényes jogalapként is értelmezhetjük arra, hogy a rendszert folyamatosan ellenőrizzük, a hálózati adatforgalmat naplózzuk.

Az is felmerülhet az állami és önkormányzati szervek elektronikus információbiztonságáról szóló 2013. évi L. törvény hatálya alá tartozó szervek esetében, hogy adatgyűjtésük céljaként a törvénynek való megfelelést nevesítsék, ennek érdekében pedig – már az *érdekmérlegelés* jogalapját segítségül hívva, a szükséges érdekmérlegelési tesztet elvégezve – viselkedéselemzést alkalmazzanak.

Számos kérdés merülhet fel azonban a munkaviszonyhoz, tagsági viszonyhoz kötődő profilozás kapcsán, amelyeket munkajogi és adatvédelmi jogi szempontból is szükséges vizsgálnunk. Amennyiben egy szervezet munkavállalóinak monitorozásáról beszélünk, akkor a rendszer által gyűjtött adatok és az abból levonható következtetések (úgynevezett prediktív profil) szükségszerűen kiegészíthetővé válnak az offline világból rendelkezésre álló adatokkal, így a felhasználók még pontosabb beazonosítását teszik lehetővé (explicit profil). Ha a munkáltató nem csak metaadatokat, hanem a kommunikáció tartalmát is vizsgálja – például kártékony kódok terjedésének, vagy üzleti titkainak szivárgását megelőzendő –, akkor fennáll a veszélye annak is, hogy olyan különleges adatok (egészségügyi állapot, szexuális érdeklődés, pártállás, vallás stb.) is az adatkezelő tudomására jutnak így, melyeket jogszerűen nem kezelhet. A beérkező kommunikáció vizsgálata szintén problémát vethet fel, hiszen feladójának személyes adatai is veszélybe kerülhetnek, aki nem járulhatott hozzá az adatgyűjtéshez, nem kaphatott tájékoztatást az adatkezelésről (Bankó és Szőke 2015).

Fentiek, és a NAIH jogértelmezése alapján munkaviszonyhoz kapcsolódóan az érintett saját profilozásához való hozzájárulása nem tekinthető megfelelő jogalapnak, hiszen alárendeltségi viszonyából következően, döntése esetleges következményei miatt nem tudja önkéntes, befolyástól mentes hozzájárulását adni az adatkezeléshez.

A munkáltató jogos érdekeire tekintettel azonban szigorú garanciák érvényesülése mellett mégis ellenőrizhető az internethasználat és a munkahelyi eszközök adattartalma, ha az törvényi rendelkezésen, illetve megfelelő érdekmérlegelésen, valamint előzetes tájékoztatáson alapul. A NAIH munkahelyi adatkezelések jogszerűségéről szóló 2016 novemberi tájékoztatója kitér az internethasználat ellenőrizhetőségére is. A NAIH jogértelmezése szerint a Munka Törvénykönyvéről szóló 2012. évi I. törvény 11. §-a megfelelő jogalapot ad a munkáltatónak, hogy ellenőrizze a munkavállaló online tevékenységét, és adott esetben munkajogi jogkövetkezményt alkalmazzon a munkavállalóval szemben. Az ellenőrzés eszközének kiválasztásához és kereteinek meghatározásához a munkáltatónak el kell végeznie az érdekmérlegelés tesztjét, valamint meg kell határoznia, hogy milyen

[13] A követelményekről lásd az Adatvédelmi Munkacsoport az elektronikus kommunikáció hírszerzési és nemzetbiztonsági célú megfigyeléséről szóló 4/2014. számú véleményét (WP 215), valamint az azt alátámasztó jogi értékelését (WP 228).

céllal, milyen érdekei mentén ellenőrzi az internethasználatot. Fontos elvárás, hogy az ellenőrzés kereteit megadó belső szabályzatot készítenie, és az ellenőrzésnek a munkavállaló munkaköréhez igazodónak kell lennie. A munkáltatónak kötelessége a munkavállalót részletesen tájékoztatni az ellenőrzés előtt, és a vizsgálat csupán arra terjedhet ki, hogy a munkavállaló betartotta-e a belső szabályzatokban rögzített munkáltatói rendelkezést (tiltott oldalak, vagy kommunikáció, például chat), tehát a munkavállaló részletes tevékenységének feltérképezése nem megengedett.

Álláspontunk szerint a NAIH által meghatározott – munkáltatói ellenőrzési célú, és teljesítményméréshez kötődő – ellenőrzéshez képest közvetlenebb gazdasági érdeke fűződik a munkáltatónak a biztonsághoz. Ezért a fenti korlátok ellenére a védelmi célú profilozás érdekmérlegelési tesztje megengedőbb eredményt hozhat. Boehm, Hey és Ortner (2016) egy jogszerűen kialakított viselkedéselemzési megoldás (biztonságtudatossági teszt) bemutatása kapcsán felhívja a figyelmet arra, hogy a profilozás korlátait és feltételeit meghatározó jogszabályi felhatalmazás hiányában is lehetőséget ad az uniós adatvédelmi jog arra, hogy – az adatkezelésre vonatkozó alapelvek és előírások betartása mellett – az adatkezelő jogos érdekének érvényesítése céljából gyűjtse az adatokat. Ehhez szükséges, hogy az adatok gyűjtését a lehető legszűkebb körben és ideig végezze a munkáltató, majd ezt követően azokat álnevesítve, vagy anonim formában értékelje, és eltérő célból azokat ne használja fel.

Az új adatvédelmi szabályozás

Az EU adatvédelmi reformjának eredményeként 2012-től érezhetően nőtt az adatvédelmi szabályozás jelentősége Európában. Ezt nem csak a formálódó rendeletszöveghez kapcsolódó lobbitevékenység (Nielsen 2013a), illetve a rendelet-tervezethez az Európai Parlament fennállása óta érkezett egyik legtöbb módosító javaslat beérkezése mutatta (Nielsen 2013b), hanem az is, hogy az Európai Unió Bírósága számos nagy horderejű döntésben terjesztette ki az adatvédelmi jog hatályát.[14] A tagállamonként eltérő módon átültetett EU adatvédelmi irányelv (95/46/EK) helyébe 2018. május 25-én az EU Általános Adatvédelmi Rendelete[15] lép, amely közvetlenül alkalmazandó jogszabályként egységesen magas elvárásokat határoz meg a megfigyelést és profilozást végző adatkezelőkre szerte Európában. Újdonság, hogy hatálya nemcsak az itt működő szervezetekre, de az EU-n kívüli adatkezelőkre is kiterjed, ha az Unióban tartózkodó érintetteknek nyújtanak szolgáltatást, vagy árusítanak terméket, illetve, ha az érintettek viselkedésének megfigyelése érdekében kezelnek róluk adatokat – feltéve, hogy az Unió területén belül tanúsított viselkedésükről van szó (Rendelet 3. cikk (2)).

[14] Lásd a C-131/12. Google Spain v AEPD and Mario Costeja Gonzalez ügy az elfelejtődéshez való jogról, illetve a C-362/14. számú Maximilian Schrems v Data Protection Commissioner ügyben hozott határozatát, melyben a Snowden-ügyet követően kimondta, hogy az Egyesült Államok nem minősül adatvédelmi szempontból biztonságos harmadik országnak, és a Safe Harbor keretrendszert érvénytelennek nyilvánította.

[15] Az Európai Parlament és a Tanács (EU) 2016/679 rendelete (2016. április 27.) a természetes személyeknek a személyes adatok kezelése tekintetében történő védelméről és az ilyen adatok szabad áramlásáról, valamint a 95/46/EK rendelet hatályon kívül helyezéséről (a továbbiakban: Rendelet).

A Rendelet már egyértelműen adatkezelésként nevesíti a profilozást (4. cikk 4. pont), és személyes adatként az IP-címet, böngésző sütiket és a helymeghatározó adatokat is, csakúgy, mint a naplóállományokat, amennyiben azok egyéb információkkal összekapcsolva felhasználhatóak a természetes személyes profiljának létrehozására és az adott személy azonosítására (30. Preambulum).

A Rendelet is átveszi a jogos érdeket, mint adatkezelési jogalapot. Erre alapozva jogszerűnek nyilvánítja az olyan mértékű információbiztonsági célú személyes adatkezelést, „amely a hálózati és informatikai biztonság garantálásához feltétlenül szükséges és arányos, vagyis adott titkossági szinten az érintett hálózat vagy információs rendszer ellenálló képessége az e hálózatokon és rendszereken tárolt vagy továbbított adatok, valamint az e hálózatok és rendszerek által nyújtott vagy rajtuk keresztül elérhető kapcsolódó szolgáltatások hozzáférhetőségét, hitelességét, integritását és bizalmas jellegét sértő véletlen eseményekkel, illetve jogellenes vagy rosszhiszemű tevékenységekkel szemben." (49. Preambulum).

A monitorozás céljától függetlenül a jogos érdek csak akkor állapítható meg, ha az érintett észszerűen számíthat arra, hogy adatkezelésre az adott célból a személyes adatok gyűjtésének időpontjában és azzal összefüggésben kerülhet sor, tehát már előre tudnia kell a profilalkotási eljárások alkalmazásáról. Széles körű hozzáférési (tájékoztatási) jogot kap az érintett a profilozáshoz kapcsolódva, ám a jelenlegi szabályoknál kevesebb eszköze lesz az ellen fellépni az érdekmérlegelés következtében. Amennyiben a profilalkotás során kialakult eredményre olyan döntés épül, ami az érintett helyzetét jelentős mértékben érinti (például munkáltatói döntések), akkor a tevékenység megkezdése előtt kötelező lesz az adatvédelmi hatásvizsgálat (35. cikk) lefolytatása is. A Rendelet ugyanakkor számos adatbiztonsági előírást tartalmaz (32. cikk), valamint javasolja az álnevesítés alkalmazását, ami azonban nem vezethet arra az eredményre, hogy a továbbiakban ne minősülne az adat személyes adatnak.

A Rendelet nem alkalmazható a bűnügyi és igazságügyi célú adatkezelésekre (2. cikk). A bűnügyi és igazságszolgáltatási célú adatkezelések szabályait rögzítő 680/2016 (EU) irányelv[16] már egységes szabályokat állapít meg az EU valamennyi bűnüldöző szerve számára, míg korábban ezen a területen csak a határon átnyúló adatáramlást szabályozták. A Bűnügyi irányelv 11. cikk (1) bekezdése kimondja, hogy „az olyan, kizárólag automatizált adatkezelésen – ideértve a profilalkotást is – alapuló döntés, amelynek joghatása az érintettre nézve hátrányos vagy őt jelentős mértékben érinti, tilos, kivéve, ha (…) uniós vagy tagállami jog teszi lehetővé, amely az érintettek jogaira és szabadságaira vonatkozó megfelelő garanciákról is rendelkezik, ideértve legalább az érintett jogát arra, hogy az adatkezelőtől emberi beavatkozást kérjen."

A nemzetbiztonsági és honvédelmi célú adatkezelések a fenti jogszabályok hatályán kívül esnek, továbbra is tagállami jog alá tartoznak majd.

[16] Az Európai Parlament és a Tanács (EU) 2016/680 irányelve (2016. április 27.) a személyes adatoknak az illetékes hatóságok által a bűncselekmények megelőzése, nyomozása, felderítése, a vádeljárás lefolytatása vagy büntetőjogi szankciók végrehajtása céljából végzett kezelése tekintetében a természetes személyek védelméről és az ilyen adatok szabad áramlásáról, valamint a 2008/977/IB tanácsi kerethatározat hatályon kívül helyezéséről (a továbbiakban: Bűnügyi irányelv).

Biztonság és/vagy magánszféra? A beépített adatvédelem elve

Az EU „Europe 2020" stratégiája keretében induló adatvédelmi reformjának egyik kiemelt célja volt a felhasználók új technológiákba és az online térbe vetett bizalmának növelése. Ennek elsődleges eszközeként a digitális ügyekért felelős biztos, Viveane Reding (2011) a személyes adatok fokozottabb védelmét és az információbiztonság erősítését, mint egymást kölcsönösen feltételező és kiegészítő garanciát jelölte meg.

A szabályozás az elvek mellett ismét figyelmet fordít a technológiai fejlődés jelentette kihívásokra, a Rendelet és a Bűnügyi irányelv is kötelezően előírja a beépített és az alapértelmezett adatvédelem elvének alkalmazását, valamint az adatvédelmi szempontú előzetes hatásvizsgálat lefolytatását a magas adatvédelmi kockázatot rejtő új adatkezelések azonosítása érdekében.

A beépített adatvédelem (Privacy by Design) elvének kidolgozása Kanada korábbi adatvédelmi biztosának, Ann Cavoukiannek a nevéhez fűződik, aki a 90-es években, főleg az Egyesült Államokban megjelenő „Surveillance by Design" felfogásra keresett választ. A megfigyelésközpontú társadalom létrehozásának elve, és a kapcsolódó törvénytervezetek azt állították[17], hogy az állampolgárok biztonsága csak a magánszférájuk védelmének rovására biztosítható. Az elv hívei szerint minél inkább figyelembe vesszük a magánszféra védelmét és az adatvédelmi elveket, annál nagyobb lesz a kockázata akár egy, a kibertérből érkező, akár egy terrorizmussal összefüggő támadásnak. A napjainkban sem idegen felfogás gyakorlati megvalósulása a közterületi kamerázás rohamos terjedése és korlátlan megfigyelési funkció integrálását jelenti a kommunikációs technológiákba olyan mértékben, amelynek segítségével a rendvédelmi szervek bármilyen adathoz hozzáférhettek (Davies 2010). A Big Data-alapú megoldások terjedésével megnőtt azon fejlesztők versenyelőnye, akik olyan rendszereket képesek előállítani, amelyekben a felügyelet az általános napi működés részét képezi, a felhasználói viselkedéselemzés költségeinek csökkenése pedig magával hozhatja az adatkezelők oldalán az elv újjászületését.

A Privacy by Design elve ezzel szemben annak a filozófiája, hogy a magánszféra-védelem és az adatvédelmi szabályozás elveit integrálni kell a különböző adatkezelő technológiák követelményrendszerébe, amely így a számítástechnikai és üzleti alkalmazások integráns részévé válik anélkül, hogy azok funkcionalitást korlátozná. Elismeri a biztonság jelentőségét, de úgy kíván eredményeket elérni, hogy közben nem sérti szükségtelenül az érintettek széles körének magánszféráját, kölcsönös előnyökre törekszik (Cavoukian 2016).

Az elv gyakorlati megvalósulásának egyik legfontosabb eleme a Székely (2008) által Privátszférát Erősítő Technológiáknak fordított „Privacy Enhancing Technologies", azaz PETs-ek fejlesztése, alkalmazása, és azok terjedésének elősegítése.

A PETs kifejezésre nem található általánosan elfogadott meghatározás, leggyakrabban azonban az egyén identitását, személyazonosságát védő technikai és szervezeti megoldások gyűjtőneveként alkalmazzák (London Economics 2010). Az adatszivárgások, visszaélési botrányok magas száma jól mutatja, hogy önmagában a szabályozás, önszabá-

[17] Az érvek 1994-ben az Egyesült Államok "Communications Assistance for Law Enforcement Act" (CALEA) című törvényének vitájakor, majd a digitális távközlési hálózatok lehallgatását szabályozó 1999-es törvényjavaslat kapcsán is felmerültek. http://w2.eff.org/Privacy/Surveillance/CALEA/1999/

lyozás és a jogalkalmazás sem tudnak elegendő védelmet nyújtani a felhasználóknak a tömegesen előforduló visszaélésekkel szemben. Ugyanakkor az adatkezelők sem lehetnek biztonságban az egyre újabb, a személyes adatok megszerzésére tervezett műszaki és Social Engineering típusú támadások ellen, pedig az adatbiztonság garantálása a Rendelet hatályba lépésével (32. és 33. cikk) égető problémaként jelenik meg.

A PET-ek alkalmazásának különös jelentősége van minden olyan technológiai fejlesztés során, amelyek esetében magányszemélyek (érintettek) személyes adatait gyűjtik, elemzik, hasznosítják, tehát adatkezelés történik. E technológiák és eszközök alapvető célja, hogy ne csak az adatokat információbiztonsági szemszögből, hanem az adatalanyokat, az érintetteket is védjék a visszaélések ellen, és elősegítsék az információs önrendelkezéshez való joguk érvényesíthetőségét, ami Goldberg (2002) szerint a jogi előírások és az önszabályozás mellett a technológia által is elősegíthető lehet. Az elmúlt két évtizedben a beépített adatvédelem elve és az azt gyakorlatba átültető megoldások lassan terjedtek, létjogosultságukat azóta is sokan kétségbe vonják. Ennek egyik fő oka – a felhasználók adatvédelmi tudatosságának és ahhoz kapcsolódó aktivitásának alacsony szintje mellett (Szőke 2015) – a kötelező alkalmazásukat előíró jogszabályok hiánya volt (London Economics 2010).

Szőke és Böröcz (2013) a Privacy by Design elvének uniós átültetése kapcsán kiemeli, hogy az eredetileg a PETs megoldásokhoz kapcsolódva megjelenő, kifejezetten a technológiára fókuszáló elv a Rendeletben (25. cikk) és a Bűnügyi irányelvben (20. cikk) már átfogóan, a tervezési, üzleti, és üzemeltetési folyamatokban is kötelezően megvalósítandó előírás. Gyakorlati alkalmazása azonban továbbra is bizonytalanságot okoz, mivel a megfogalmazott elvek sokkal inkább egy szemléletet, hozzáállást tükröznek, mintsem olyan normatív követelményrendszert, amelynek betartása vagy be nem tartása könnyedén megállapítható, mérhető volna (Davies 2010).

Az elv tartalmának kidolgozása a tagállamok adatvédelmi hatóságaira hárul majd, de a beépített adatvédelem megvalósításának (Privacy Engineering) területével foglalkozó mérnökök, informatikusok már több területen is szép eredményeket értek el az álnevesítés alkalmazásával.[18] Az információbiztonsági célú felhasználói viselkedéselemzést támogató megoldások esetében is fontos cél lehet ezért a magánszféra védelmét garantáló, de ugyanakkor az elvárt biztonsági szintet még nyújtó PET-ek fejlesztése, kidolgozása.

Összefoglalás

A felhasználói viselkedéselemzés kiváló lehetőség az új típusú kiberbiztonsági kihívások kezelésére, de különös figyelmet kell fordítani annak adatvédelmi aspektusaira is. Pardo és Siemens (2014) gyűjtése alapján a következő etikai és adatvédelmi elvek mentén lehet a gépi tanulást hadrendbe állítani.

- Transzparencia: a megfigyelteknek tisztában kell lenniük azzal, hogyan működik az elemzési eljárás, és azzal, hogy milyen információkat használnak fel ennek során.

[18] Lásd az okos mérők alkalmazása során a villamosenergia-szektorban, a budapesti Groupama Aréna beléptetőrendszerének hash kóddal átalakított biometrikus beléptető adatai esetében, vagy Cavoukian (2011) összefoglalójában a nemzetközi eredményekről.

- Kontroll az adatok felett: a megfigyeltnek lehetőséget kell biztosítani arra, hogy hozzáférhessen és korrigálhassa a róla gyűjtött adatokat.
- Hozzáférési jogok: egyértelműen meg kell határozni, hogy ki és milyen körülmények között férhet hozzá és használhatja fel a gyűjtött adatokat.
- Elszámoltathatóság és ellenőrzés: egyértelműnek kell lennie, hogy ki és milyen felelősséggel bír a folyamatban.

Problémát jelenthet, hogy bár a 2018-ig alkalmazandó európai és hazai jog nem zárja ki a felhasználói viselkedéselemzésen alapuló védelmi célú mechanizmusok használatát, a tagállamok szabályozása nem egységes és az adatvédelmi hatóságok gyakorlata is különbözhet az érdekmérlegelési teszt kapcsán, így eltérő feltételekhez kötheti alkalmazásukat.

A részletszabályok kidolgozása még folyamatban van, de a Rendelet és a Bűnügyi irányelv ebben komoly változást hoz. A Rendelet már adatkezelési jogalapnak tekinti az engedély nélküli hozzáférés és a rosszindulatú programterjesztés megakadályozásához, továbbá a szolgáltatás megtagadásával járó támadások (DDOS), valamint a számítógépes és elektronikus kommunikációs rendszerekben való károkozás megállításához fűződő jogos érdeket (49. Preambulum). Az e célra fejlesztett új műszaki megoldások, szolgáltatások tervezésekor, illetve a működő rendszerek üzemeltetése során ezért mindenképpen javasolt már most figyelembe venni a Rendelet új előírásait és alapelveit is. Az érintettek megfelelő tájékoztatása mellett a beépített adatvédelem elvének megfelelően, ahol lehet, álnevesítést, PET technológiákat, valamint titkosított rendszerű kommunikációt és adattárolást alkalmazzunk.

Irodalom

A 29. cikk alapján létrehozott Adatvédelmi Munkacsoport, „2/2010. számú vélemény a viselkedésalapú online reklámról" (WP 171) 00909/10/HU, 2010.06.22. http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2010/wp171_hu.pdf

A 29. cikk szerinti Adatvédelmi Munkacsoport, „16/2011. sz. vélemény a viselkedésalapú online reklám bevált gyakorlatára vonatkozó EASA/IAB-ajánlásról" (WP 188) 2011.12. 08. http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2011/wp188_hu.pdf

A Nemzeti Adatvédelmi és Információszabadság Hatóság tájékoztatója a munkahelyi adatkezelések alapvető követelményeiről. 2016.11.15. https://www.naih.hu/files/2016_11_15_Tajekoztato_munkahelyi_adatkezelesek.pdf

Abraham, Ajith, Crina Grosan and Yuehui Chen, "Cyber security and the evolution of intrusion detection systems.", *i-Manager's Journal on Future Engineering and Technology* 1.1 (2005): 74.

Alexin Zoltán, „Does fair anonymization exist?", *International Review of Law, Computers and Technology,* Vol. 28. (2014) No. 1., pp. 21-44. http://dx.doi.org/10.1080/13600869.2013.869909

Bankó Zoltán és Szőke Gergely László, „Az információtechnológia hatása a munkavégzésre", Pécs, Utilitates Bt., (2015) pp. 55–66.

Boehm, Franziska, Tim Hey and Robert Ortner, "How to measure IT security awareness of employees: a comparison to e-mail surveillance at the workplace", *European Journal of Law and Technology,* Vol 7. (2016), No 1. http://ejlt.org/article/view/500/633

boyd, danah and Kate Crawford, "Critical Questions for Big Data", *Information, Communication & Society,* 15:5 (2012), pp. 662-679. http://dx.doi.org/10.1080/1369118X.2012.678878

Cavoukian, Ann, "Embed Privacy by Design, or Risk Losing Privacy Forever", Berkeley Center for Law & Technology, 2016. https://www.law.berkeley.edu/wp-content/uploads/2016/03/Ann-Cavoukian.pdf

Cavoukian, Ann, *Privacy by Design. Strong Privacy Protection – Now, and Well into the Future. A Report on the State of PbD to the 33rd International Conference of Data Protection and Privacy Commissioners*, 2011. https://www.ipc.on.ca/wp-content/uploads/Resources/PbDReport.pdf

Davies, Simon, *Why Privacy by Design is the next crucial step for privacy protection – A discussion paper*, 2010. http://i-comp.org/wp-content/uploads/2013/07/privacy-by-design.pdf

Dell SecureWorks, *Underground Hacker Markets*, 2016.

Goldberg, Ian, "Privacy-enhancing technologies for the Internet, II: Five years later." in Roger Dingledine and Paul Syverson (eds.), *Privacy Enhancing Technologies. Second International Workshop, PET 2002 San Francisco, CA, USA, April 14–15, 2002 Revised Papers*, Springer-Verlag, Berlin-Heidelberg-New York, 2002. http://dx.doi.org/10.1007/3-540-36467-6_1

Hutchins, Eric M., Michael J. Cloppert and Rohan M. Amin, "Intelligence-Driven Computer Network Defense Informed by Analysis of Adversary Campaigns and Intrusion Kill Chains", in Julie Ryan (eds), *Leading Issues in Information Warfare and Security Research, Vol. 1.*, Academic Conferences Limited, Reading, 2011, pp. 80-106.

International Telecommunication Union, *ICT Facts and Figures 2016*, ITU, Geneva, 2016.

Iverson, Brian, "Maverick: The Unbearable Cost of Privacy", Gartner, 2015.

Lee, Dave, "Obama presses Trump on cybersecurity", *BBC News*, 3 December 2016, http://www.bbc.com/news/technology-38193663

London Economics, *Study on the economic benefits of of privacy-enhancing technologies (PETs)*. Final Report to The European Commission DG Justice, Freedom and Security, 2010. http://ec.europa.eu/justice/policies/privacy/docs/studies/final_report_pets_16_07_10_en.pdf

Lyon, David, "Surveillance, Snowden, and big data: Capacities, consequences, critique", *Big Data & Society* Vol. 1. (2014) Issue 2., pp. 1-13. http://dx.doi.org/10.1177%2F2053951714541861

Minárik, Tomáš, "NATO Recognises Cyberspace as a 'Domain of Operations' at Warsaw Summit", Tallin, 21 July 2016, https://ccdcoe.org/nato-recognises-cyberspace-domain-operations-warsaw-summit.html

Morgan, Steve (ed.), *Hackerpocalypse: A Cybercrime Revelation*, Cybersecurity Ventures, 2016.

Nemeslaki András és Sasvári Péter László, „Az információbiztonság-tudatosság empirikus vizsgálata a magyar üzleti és közszférában", *Infokommunikáció és Jog*, 60. szám (2014), pp. 169-177.

Nemzetközi Távközlési Adatvédelmi Munkacsoport, *Webtracking és magánszféra: a kontextus, az átláthatóság és az ellenőrzés alapvető fontosságú marad*", Munkadokumentum, 53. Ülés, Prága, 2013. április 15-16. https://www.naih.hu/files/IWGDPT–Webtracking-es-maganszfera–HUN.pdf

Nielsen, Nikolaj, "MEPs copy-pasting amendments from US lobbyists", *euobserver*, 12 February 2013, https://euobserver.com/justice/119028 (2013a)

Nielsen, Nikolaj, "The man behind the EU parliament's data regulation", *euobserver*, 06 May 2013, https://euobserver.com/justice/119951 (2013b)

Ohm, Paul, "Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization", *UCLA Law Review* Vol. 57. (2010) Issue 6., pp. 1701-1777. http://www.uclalawreview.org/pdf/57-6-3.pdf

Pardo, Abelardo and George Siemens, "Ethical and privacy principles for learning analytics", *British Journal of Educational Technology*, Vol. 45. (2014) Issue 3., pp. 438-450. http://dx.doi.org/10.1111/bjet.12152

Ponemon Institute LLC, *2016 Cost of Data Breach Study: Global Analysis*, Ponemon, Traverse City, 2016.

Reding, Viviane, "The upcoming data protection reform for the European Union," *International Data Privacy Law* Vol 1. (2011) Issue 1., pp. 3-5. https://doi.org/10.1093/idpl/ipq007

Székely Iván, „Jog ahhoz, hogy elfelejtsenek és töröljenek”, *Információs Társadalom* XIII. évfolyam (2013) 3-4. szám, 7-27. old. http://www.infonia.hu/digitalis_folyoirat/2013/2013_34/i_tarsadalom_2013_34_szekely.pdf

Székely Iván, „Privátszférát erősítő technológiák”, *Információs Társadalom*, VIII. évf. (2008) 1. szám, 20-34. old.

Szőke Gergely László és Böröcz István, „A beépített adatvédelem (privacy by design) elve”, *Infokommunikáció és Jog,* 56. szám (2013), 120-125. old.

Szőke Gergely László, *Az európai adatvédelmi jog megújítása. Tendenciák és lehetőségek az önszabályozás területén*, HVG-ORAC, Budapest, 2015.

Tamásné Szabó Zsuzsanna, „Nemcsak a Budapest Bank, több hazai nagybank ügyfeleitől is loptak pénzt”, *24.hu*, 2015. augusztus 13. http://24.hu/fn/penzugy/2015/08/13/tobb-hazai-nagybank-ugyfeleitol-is-loptak-penzt-a-kartyacsalok/

Dr. Kiss Attila infokommunikációs szakjogász, korábban a Nemzeti Közszolgálati Egyetem Államtudományi és Közigazgatási Karának oktatója. Jogász diplomáját 2011-ben szerezte a Pécsi Tudományegyetemen, 2009-ben az Egyesült Királyságban a Coventry University (Erasmus), majd 2010-ben Csehországban a brnoi Masaryk Egyetem (Visegrad Fund ösztöndíj) hallgatója volt. 2011 és 2014 között a PTE ÁJK Informatikai és Kommunikációs Jogi Tanszékének doktorandusz hallgatója, témavezetője Balogh Zsolt György. Kutatási területe elsősorban a személyes adatok és a képmás védelme, több tanulmánya vizsgálja a térfigyelő kamerázás jogi hátterét és az Európai Unió adatvédelmi reformját.

Dr. Krasznay Csaba, PhD okleveles villamosmérnök, a katonai műszaki tudományok doktora, jelenleg a Nemzeti Közszolgálati Egyetem Államtudományi és Közigazgatási Karának adjunktusa. MSc diplomáját a Budapesti Műszaki és Gazdaságtudományi Egyetemen szerezte 2003-ban, PhD fokozatát a Nemzeti Közszolgálati Egyetem Katonai Műszaki Doktori Iskolája bocsátotta ki 2012-ben. Korábban kutatóként dolgozott a Budapesti Műszaki és Gazdaságtudományi Egyetemen, valamint információbiztonsági tanácsadóként, szakértőként több mint 10 éves tapasztalata van a kiberbiztonság üzleti világából. 2011-ben az Év Útmutató IT Biztonsági Szakemberének választották. Kutatási területe a kiberbiztonság és az elektronikus közszolgálati rendszerek információbiztonsággal kapcsolatos kérdései.