VESZELSZKI ÁGNES

Adatvédelmi paradoxon vs. adatbiztonság. Előszó az Adatbiztonság számhoz

„Csak két »iparág« nevezi az ügyfeleit usereknek, azaz (fel)használóknak: a közösségi média és a drogkereskedelem" – hangzik el a 2020 őszén nagy (virtuális) port kavart *Társadalmi dilemma* (*The Social Dilemma*) című dokumentumfilmben, amelyben éppen az oldalak alkotói, tervezői, szerkesztői vallanak arról, hogy a közösségimédia-függőség, az oldalak addiktivitása tudatos tervezés eredménye. A legfrissebb statisztikák[1] szerint az emberiség nagyjából fele, azaz több mint négy és fél milliárd ember van jelen valamely közösségi platformon. Nem túlzás tehát azt állítani, hogy a közösségi média folyton változó algoritmusai – és általuk ezen oldalak tulajdonosai, szerkesztői – igen erős kontrollt képesek gyakorolni az emberiség nagy részének figyelme, informálódási szokásai, tartalomelérése és – legegyértelműbben – adatai fölött. A közösségi oldalak mellett az ugyancsak a *big data* használatára építő, további digitális technológiák is fontos adatvédelmi és biztonsági kérdéseket vetnek föl. Amikor a felhasználók az elektronikus eszközeiket használják, adatokat hoznak létre, amelyekre építve minden esetben (tudatos vagy nem szándékolt) felhasználói megfigyelés folyik. Erre utal Smith és Kollars „ellenőrizetlen elektronikus panoptikum" (*uncontrolled electronic panopticism*) fogalma.[2] Ám miközben a felhasználók rendszeresen aggodalmukat fejezik ki az online (létrejövő, tárolt) adataik biztonsága miatt, nagyon keveset tesznek ténylegesen a személyes adataik védelme érdekében. Ezt az attitűd és valós viselkedés közötti diszkrepanciát nevezi a szakirodalom[3] adatvédelmi paradoxonnak (*privacy paradox*).

A *Századvég* folyóirat 2022. évi első száma ennek a témakörnek jár utána több nézőpontból: a társadalom- és jövőkutatás, a kiberbiztonság,

[1] Kemp, Simon 2022: *Digital 2022: Global Overview Report.* 2022. január 22. https://datareportal.com/reports/digital-2022-global-overview-report

[2] Smith – Kollars 2015, 160.

[3] Összefoglalásuk: Barth – de Jong 2017.

a jog és szabályozás, illetve a kommunikációkutatás területei felől. Az itt bemutatott hat cikk célja, hogy szakterületeken átívelő áttekintést adjon az automatizáció, az adatkapitalizmus és az adatbiztonság témakörének aktuális kihívásairól.

A tematikus szám nyitótanulmánya, *Kontrollforradalom, adatvezéreltség és megfigyelési kapitalizmus* címmel, James Beniger nyomán a társadalom történetét kontrollforradalmak sorozataként láttatja, amelyben a legutóbbi fejlemény a (Beniger által a legtöbb szerzőtől eltérően már a 19. század közepére datált) információs társadalom, illetve az ehhez kötődő legújabb ellenőrzési forradalom. „Mára [...] eljutottunk odáig, hogy valós idejű adatgyűjtésen alapulva, akár automatizált módon, algoritmusok segítségével, de (egyelőre) emberi ellenőrzés mellett lehet igen komplex pénzügyi, gazdasági, média- vagy egyéb rendszereket távolról is menedzselni" – állítja a cikk szerzője, Pintér Róbert. A tanulmány tisztázza az adatvezérelt kapitalizmus, a megfigyelési kapitalizmus fogalmát, miközben olyan jelenségekre, „externáliákra" is kitér, mint a sokat vitatott visszhangkamra (*echo chamber*), illetve a szűrőbuborék (*filter bubble*) jelensége. A cikk az összegzésében kitekint a legújabb európai uniós fejlesztésekre, illetve a magyar cégek helyzetére is.

Szinte ezt a gondolatmenetet folytatja Krasznay Csaba *Adatok és automatizáció a kiberbiztonság szemszögéből* című tanulmánya, amely a jelen korunkat a negyedik ipari forradalom, illetve az ebbe illeszkedő adatkapitalizmus fogalmával írja körül, és a 21. századot az adatok évszázadaként jellemzi, amelyben „az adat az új olaj". A cikk a legfontosabb kiberbiztonsági kihívásokat rendszerezi, miközben az ezekre jelenleg érvényes megoldási lehetőségeket is felmutatja. A kiberfenyegetések főbb aktorai közé a kiberbűnözői csoportok, a kiberkémek, a kiberterroristák és a kiberhadviselést művelő haderőnemek tartoznak. A legjellemzőbb fenyegetések pedig a szerző szerint a zsarolóvírusok és a túlterheléses támadások, a kémprogramok, a kriptovalutákhoz kötődő csalások, az e-mailen keresztüli visszaélések, illetve legújabban az információs hadviselés, a dezinformáció – miközben mindezek használata során egyre erőteljesebben szerepet kap az automatizáció, a mesterséges intelligencia használata is. Ugyan a kiberbiztonsági rabló-pandúr harcban a támadók mindig a védelem előtt járnak, ám az „incidensmenedzsmentben felhasznált informatikai megoldások szédületes fejlődése néhány év alatt tette versenyképessé a kibervédelmet a támadókkal szemben" – állítja a tanulmány.

Az eddigiekben is tárgyalt automatizálás és annak szabályozása számos jogi kérdésben „gyors megoldásra vár" – állítja Sulyok Márton és Mercz Mónika, hiszen az automatizálás számos adatvédelmi és más emberi jogi aggályt vethet fel. Az *Adatok és automatizáció – atipikus vagy archetipikus veszélyek?* című cikk áttekinti, hogy az automatizáció fogalmának milyen kapcsolata van az adatokkal és az adatvédelemmel, illetve bemutatja a terület alapvető jogi kereteit és a jövőbeli szabályozási kihívásokat is.

Az archetipikus és atipikus veszélyek ismertetése után következik Miklós Gellért tanulmánya az Európai Unió adatstratégiájához kapcsolódó jogszabályi keretrendszerről. A cikk bemutató összefoglalást kínál az általános adatvédelmi rendeletről (GDPR) – ehhez kötődően a személyes adatok köréről, a harmadik országba történő adattovábbításról; továbbá az adatrendelet tervezeteiről (*Data Act*), a nem személyes adatok Európai Unióban való szabad áramlásáról szóló rendeletről (FFD), illetve a kiberbiztonsági rendeletről (CSA). A tanulmány jogi szempontból reflektál a globális digitális gazdasági versenyre és abban az EU helyzetére.

Ugyancsak kifejezetten európai uniós kontextusban vizsgálja az automatizáció jogi szabályozási lehetőségeit Eszteri Dániel és Péterfalvi Attila az *Amikor a gépeink tanulnak minket: avagy a mesterséges intelligencia alapú döntéshozatal és profilozás szabályozásának európai uniós törekvéseiről* című tanulmánya. A hétköznapokban is sokat emlegetett, európai uniós adatvédelmi rendelet (GDPR) alapján elemzi a szerzőpáros a gépi tanulásra alkalmas, vagyis az automatizált döntések meghozatalára képes szoftverek jogi megfeleltethetőségét. A témakör adatbiztonsági összefüggéseire egy, a Cambridge Analytica-botrányt taglaló esettanulmányon keresztül mutatnak rá a szerzők. A cikk egy új, EU-s mesterségesintelligencia-kódex tervezetének bemutatásával zárul, amely például a társadalmi pontozórendszerek, a biometrikus azonosítók használatának, a csevegőrobotok szabályozását is magában foglalja.

Ez utóbbi témakör, a kommunikációra képes robotok, a virtuális influencerek világa adja Horváth Evelin vizsgálati tárgyát. A *Pixelekbe öntött érzelmek. A virtuális érzelemmegjelenítés vizsgálatának lehetőségei* című tanulmány a virtuális (android, azaz emberszerű) karakterek érzelemmegjelenítésének lehetőségeivel, a virtuális figurák humanizálásával foglalkozik a szisztematikus szakirodalmi áttekintés módszerével, és bemutatja a kutatókat, fejlesztőket nyugtalanító *uncanny valley*-jelenséget is. A virtuális karakterek digitális-vizuális produktumokként ugyancsak adatok-

ra épülnek: adatok keletkeznek a létrehozásukkor, a (felhasználó vagy az alkotó által történő) módosításukkor, a (marketing-, videójáték-, oktatási vagy egyéb célra) felhasználásukkor – sőt az érzelemkifejezés elemzésekor adatokra épít az emberi szemlélő számára hitelesnek tűnő arckifejezéseket megalkotó mesterséges intelligencia is.

Az adatvédelmi paradoxon a kutatások szerint a kockázat és a bizalom közötti egyensúlykeresésben rejlik, amely folyamatnak igen lényeges összetevője az informáltság. Az adatbiztonságról szóló folyóiratszám szerkesztőjeként abban a reményben adom át a tisztelt Olvasóknak ezt az egy logikai láncra fűzhető tanulmánygyűjteményt, hogy az ebből is származó informáltság révén még tudatosabb internethasználókká és adatkezelőkké válhatnak.

Irodalom

Barth, Susanne – de Jong, Menno D. T. 2017: The privacy paradox – Investigating discrepancies between expressed privacy concerns and actual online behavior. A systematic literature review. *Telematics and Informatics,* Volume 34, Issue 7, 1038–1058. https://doi.org/10.1016/j.tele.2017.04.013.

Smith, E. J. – Kollars, N. A. 2015: QR panopticism: user behavior triangulation and barcode-scanning applications. *Information Security Journal: A Global Perspective,* Volume 24, Issue 4–6, 157–163.