DOI: https://doi.org/10.12700/btsz.2026.8.2.99

ARTIFICIAL INTELLIGENCE AND USER PROFILING: OVERVIEW AND RISKS

MESTERSÉGES INTELLIGENCIA ÉS FELHASZNÁLÓI PROFILALKOTÁS: HELYZETKÉP ÉS KOCKÁZATOK

BOKROS Anna Dóra[1]

Abstract

The study reviews the current state of AI-based user profiling, the major related events, and the regulatory environment, with particular attention to legislative gray areas, user awareness, and the possibilities for targeted manipulation inherent in the technology. It highlights that user profiling, based on the analysis of data collected across various digital systems, can be used not only for cybersecurity or marketing purposes, but also for optimizing attacks and targeted opinion manipulation. Furthermore, it draws attention to the role of behavioral biometric data processing in user profiling, the composition of users' digital footprints, and the shortcomings and dark patterns used in informing users about the handling of their data.

Keywords

user profiling, targeted opinion manipulation, AI regulation, AI-driven profiling, user digital awareness, GDPR, anonymization, dark patterns

Absztrakt

A tanulmány áttekinti a mesterséges intelligencia szerepét a felhasználói profilalkotásban, a kapcsolódó jelentősebb eseményeket és az európai szabályozási környezetet, különös tekintettel a jogalkotói szürke zónákra, valamint a felhasználók tudatosságára és a technológiában rejlő célzott manipulációs lehetőségekre. Rávilágít, hogy a felhasználói profilalkotás során gyűjtött adatok elemzése által nyert adatok a kiberbiztonsági, vagy marketingcélú felhasználás mellett akár támadások optimalizálására, célzott véleménybefolyásolásra is. Felhívja a figyelmet továbbá a viselkedés alapú biometrikus adatok kezelésének felhasználói profilalkotásban betöltött szerepére és a felhasználók digitális lábnyomának összetételére, valamint a felhasználók tájékoztatásában alkalmazott hiányosságokra, sötét mintázatokra.

Kulcsszavak

felhasználói profilalkotás, véleménybefolyásolás, MI rendelet, MI vezérelt profilalkotás, felhasználók digitális tudatossága, GDPR, anonimizálás, sötét mintázatok

[1] bokrosdora@gmail.com | ORCID: 0009-0001-8436-5626 | Had-és biztonságtechnikai mérnök, Okleveles biztonságtechnikai mérnök | Óbudai Egyetem Bánki Donát Gépész és Biztonságtechnikai Mérnöki Kar Mesterséges Intelligencia Műhely | Military and Security Engineer, Certified Security Engineer | Óbuda University Bánki Donát Faculty of Mechanical and Safety Engineering Artificial Intelligence Workshop

A FELHASZNÁLÓI PROFILOK ADATÖSSZETÉTELE

A felhasználói profilalkotás gazdasági és politikai jelentősége

A felhasználói profil a felhasználók, vagy felhasználói csoportok eszköz, demográfiai és viselkedési adatainak, preferenciáinak gyűjteménye és az azokból feldolgozás során nyert következtetések, melyek nagy pontossággal leírják a felhasználók interakcióit a vizsgált alannyal kapcsolatban. A profilalkotás magában foglalja a felhasználók egy adott szoftver, szolgáltatás, platform vagy egyéb termékkel kapcsolatos interakcióhoz kötődő adatainak gyűjtését, elemzését és egyéb adataihoz való társítását, melyet különböző ágazatok használnak fel, első sorban személyre szabott felhasználói élmény tervezésére, termékfejlesztésre, valamint hatékony marketingstratégiák kialakítására. A felhasználói viselkedés monitorozásának piacát nem könnyű egységes piacként definiálni, mivel egymást átfedő analitikai rétegek ökoszisztémája, ugyanakkor globális értékét 2025-ben hozzávetőleg 3.1 milliárd USD-re becsülték, mely 2026 első felére 3,61 milliárdra növekedett, emellett egyes előrejelzések alapján 2031-re 7,65 milliárdra, [1] mások szerint 2030-ra 13,6 milliárd USD-re fog nőni. [2] Több ezer szolgáltató kínál jelenleg marketing célú felhasználói profilalkotásra szolgáló termékeket az egyszerű adatelemző eszközöktől a komplex valós időben frissülő platformokig, azonban bizonyos felmérések szerint a piac hozzávetőleg 44%-át 8-10 vállalat teszi ki – mint például a Google, IBM, Oracle vagy SAS. [3] A növekedés többek között annak az igénynek köszönhető, hogy a szervezetek a statikus adatokon túlmutatóan a kontextust is számításba kívánják venni, melyhez a hiányzó láncszem a felhasználói viselkedés. Az az iparág bővülésében kulcsfontosságú tényező az ügyfelek vásárlási szokásainak és viselkedésének megértésének egyre növekvő szükségessége, valamint az olyan fejlett technológiák megjelenése, mint a mesterséges intelligencia (MI), a gépi tanulás (ML) és az üzleti folyamatok automatizálása. [4]

Az MI fejlődése és elterjedése mellett 2020-as évek másik meghatározó eseménye, hogy a COVID-19 járvány következtében az emberek élettere jelentős mértékben a digitális platformok és online ökoszisztémák irányába tolódott el. Ez felgyorsította a digitalizáció elterjedését az élet szinte minden területén, jelentős hatás gyakorolva a munkaszervezésre, oktatásra, vásárlási szokásokra, kapcsolattartásra, miközben előre látható és előre nem látható lehetőségek, kihívások is megjelentek. [5]

A fejlődés másik fő ösztönzőereje a világban jelenleg zajló fegyveres konfliktusok hatására kibontakozó fejlesztési verseny. A mesterséges intelligencia kettős felhasználású technológia. Alkalmazása mindent felgyorsít – a döntéshozatalt, az eszkalációs ciklusokat, a detektálást és a támadásokat is. A célpontokról gyűjtött és következtetett információk minőségének javulása hatására a felderítéstől a megsemmisítésig tartó folyamat jelentősen lecsökkenthető. A felhasználók profilozása során felhalmozott és elemzett adatok nem csupán a marketingszakemberek számára képviselnek hatalmas értéket, hanem kibervédelmi, bűnüldözési, politikai stratégiai jelentőséggel is bírnak. Olyan eszközök, amelyek korábban csak a kormányokra vagy világvezető vállalatokra korlátozódtak, kisebb csoportok vagy egyének számára is elérhetővé válnak. Ugyanakkor szükséges kiemelni, hogy ettől nem lesz automatikusan előnyös vagy veszélyes a technológia. Ugyanakkor – mint minden úttörő technológia esetén – jelenleg számos technikai, jogi, etikai, edukációs szürke zóna alakult ki, melyeknek lehetnek jelentős negatív hatásai ártó szándékú felhasználás, visszaélés esetén, és mely lehetőségekre szükséges kiemelt figyelmet fordítani.

A felhasználói profilalkotás mai formájához vezető út

A profilalkotás évszázados múltra visszatekintő interdiszciplináris terület. Jóval az iparosodás előtti időkre visszanyúló első formájának tekinthető a kereskedők közvetlen kapcsolata vásárlóikkal, akiknek ismerték preferenciáit, fizetési megbízhatóságát, családi hátterét. A XIX. század végén a postai rendelésre és katalógusértékesítésre épülő vállalkozások gyűjtötték az ügyfelek rendelések során megadott adatait, melyekhez demográfiai adatokat kezdtek társítani, hogy szegmentált ügyfélcsoportokat hozhassanak létre. A feldolgozás papír alapon történt matematikai módszerekkel.

A XX. század elején jelentős előrelépés jelentett a számítási kapacitás növekedésében a Herman Hollerith által kifejlesztett lyukkártya-rendszer. Az 1950-es évektől a pszichológia nagyobb szerepet kapott az ügyfélprofilozásban, melynek úttörője, Ernest Dichter pszichológus és marketingkutató interjúk, projektív tesztek és csoportbeszélgetések révén próbálta feltárni a vásárlók tudattalan indítékait. Számításba vett olyan személyiség és viselkedésbeli tényezőket mint a vágyak, félelmek, identitás, társadalmi státusz kifejezése. [6] Az 1960-as évektől megjelentek a központosított nyilvántartások, melyek a különböző szervezetek ügyfeleik hitelképességére, vásárlási szokásaira, előfizetéseire, tulajdonukban álló ingóságaikra, becsült háztartási jövedelmükre vonatkozó adatokat is társítottak az eddigiekhez.

A személyi számítógépek kora magával hozta a széleskörű felhasználói adatok decentralizált gyűjtésének és feldolgozásának új eszközeit. Az 1980–1990-es években a relációs adatbázisok megjelenésével a vállalatok elkezdték rendszerezni és tárolni az ügyféladatokat. Ekkor vált lehetővé a vásárlási előzmények és tranzakciók követése, ami jelentős előrelépést hozott a profilozásban. A személyi számítógépek elterjedésével nagyobb teret nyert a közvetlenül a felhasználók által önkéntes, explicit hozzájárulás révén megadott adatok kezelése, amelyek tipikusan regisztrációs folyamatok, kérdőívek, vagy ügyfélszolgálati interakciók során keletkeznek. Megjelentek továbbá az ügyfélkapcsolat-kezelő rendszerek, például az Oracle Siebel CRM, amelyek segítségével a vállalatok célzottabb marketingtevékenységet tudtak folytatni. A hangsúly a demográfiai adatok helyett egyre inkább a viselkedési adatokra helyeződött át.

A 1990-es évek közepétől az internet elterjedésével megjelentek a HTTP sütik, amelyek lehetővé tették a felhasználók online tevékenységének dinamikusabb követését. A különböző digitális termékek, szolgáltatások, felületek használata során automatikusan generálódó eszköz- és technikai adatok, mellett a weboldalak rögzíteni kezdték a felhasználók oldalmegtekintéseit, kattintási útvonalait és munkamenetbeli viselkedését, ami megalapozta az online viselkedésen alapuló profilozást. Az olyan cégek, mint a DoubleClick, úttörő szerepet játszottak a hirdetési célú adatgyűjtésben.

A 2000-es évek végére a vezető technológiai platformok, mint a Google és a Facebook (2021 óta Meta), hatalmas mennyiségű, több munkameneten és eszközön átívelő adatot kezdtek felhalmozni a felhasználóikról. Egyre nagyobb szerepet kaptak az érdeklődési körökre épülő célzott hirdetések. A 2010-es években az okostelefonok és a mobilapplikációk, főként közösségi média felületek elterjedése még tovább bővítette az adatgyűjtés lehetőségeit, így a profilozás egyre nagyobb mértékben támaszkodott a felhasználók kapcsolati hálózatára, online viselkedésre, alkalmazáshasználatra, közzétett tartalmakra, vélemények és reakciók valós idejű elemzésére.

A 2010-es évek végétől a 2020-as évek elejéig a Big Data és a gépi tanulás vált meghatározóvá. A profilok ekkor már folyamatosan frissülő, valószínűségi alapú rendszerekké váltak, amelyeket előrejelzések készítésére használtak.

Az MI eszközök segítségével lehetővé vált a nagy mennyiségű gyűjtött adat dinamikus, akár valós idejű elemzése és a profilok felhasználó specifikus hiper-perszonalizációja a korábban jellemző statikus demográfiai adatok elemzésén túllépve. Ezek alapján dinamikus következtetéseket lehet levonni a felhasználók hangulatára, véleményére, személyiségjegyeire, jövőbeli vásárlási hajlandóságára, egyéb döntéseire vonatkozóan is. A prediktív analízis többek között olyan módszereket használ, mint a viselkedési adat klaszterezés, trendelemzés, adaptív tanulási algoritmusok, érzelmi bevonódás mértékének mérése nyelv-feldolgozás (NLP) segítségével, vagy szolgáltatáselhagyási szándék észlelése. Az így nyert inferált adatok egyaránt felhasználhatók az online tér biztonságosabbá tételére például csalásmegelőzés céljából, szélsőséges csoportok formálódásának és aktivitásának felismerésére, ugyanakkor politikai kampánytevékenységre, hamis vagy torzított információ célzott, csoport- vagy egyénspecifikus terjesztésére is. [7] Ezt jól szemlélteti a 2018-as Facebook–Cambridge Analytica botrány, mely során a brit politikai elemző vállalat egy ártatlannak tűnő alkalmazáson keresztül hozzávetőleg 87 millió Facebook felhasználó adatait gyűjtötte össze tudomásuk és hozzájárulásuk nélkül, majd ezeket pszichográfiai profilalkotásra és célzott politikai befolyásolásra használták, többek között a 2016-os amerikai elnökválasztási kampány során. [8] Az olyan eszközök fejlődésén túlmenően, mint a webes adatkinyerés (web scraping), adatösszekapcsolás (data linking), vagy a nyelvi tanulási modellek által elemzett felhasználói tartalmak mellett az MI alapú chat applikációk további adatgyűjtési lehetőségeket és adatvédelmi kihívásokat hoztak magukkal.

Az MI fejlődése magával hozta a felhasználók élete több aspektusának gyökeres változását, valamint edukációs hiányosságokat is. Így az MI chatbot felhasználók jelentős része amellett, hogy a munkahelyi korlátozások ellenére napi feladatai egy részét végeztetik el a chatbotokkal, gyakran adnak meg személyes adatot, vagy rájuk utaló információt, illetve egészségügyi állapotukra vonatkozó tanácsot, diagnózist kérő lekérdezéseket visznek be, emellett egyre nő azok száma, akik pszichológiai segítséget kérnek a chatbotoktól, vagy a társas kapcsolataikat helyettesítik mesterséges intelligenciával, jelentős adatvédelmi kockázatnak téve ki magukat. Csak az elmúlt évben több MI chat prompt szivárgással kapcsolatos eset kapott nyilvánosságot. 2025 augusztusában a Google több ezer megosztott ChatGPT beszélgetést indexelt, így azok kereshetővé és nyilvánosan hozzáférhetővé váltak. Az indexelt oldalak teljes csevegési előzményeket tartalmaztak – beleértve az érzékeny, privát és korlátozott terjesztésre szánt adatokat is. [9] Egy másik esetben 2025 szeptemberében a Google Search Console lekérdezései között esetenként 300 karakternél hosszabb ChatGPT felhasználói lekérdezések is megjelentek, melyeknél több esetben a felhasználók magánéleti helyzetüket fejtették ki az applikációnak. [10] Az rendszerek, mint a ChatGPT, képesek felhasználói adatok kinyerésére és osztályozására az interakcióik alapján. Az OpenAI szerint a felhasználóknak továbbra is joguk van elutasítani az adataik felhasználását a modell fejlesztéséhez, viszont rendszeresen kritika éri a szervezetet a nem kellőképpen transzparens adatkezelési gyakorlatok miatt. [11] [12]

A viselkedésalapú adatok egy speciális kategóriáját képzik az olyan biometrikus adatok, mint a kattintások, érintések, görgetések, billentyűleütések ritmusa, képernyő mé-

reteihez viszonyított helyzete, nyomáserőssége, lenyomás ideje, bizonyos esetekben beszédhang elemzése, illetve egyéb viselhető okoseszközök által gyűjtött egészségügyi adatok, mint például a szívverés vagy járásdinamika. Mivel a viselkedésalapú biometrikus adatok feldolgozása a folyamatosan zajlik a háttérben és nem igényli a felhasználó aktív közreműködését, valamint nem az emberi test időben állandó fizikai attribútumainak rögzítésén alapul, elfogadottsága magasabb a felhasználók körében. [13] A felhasználói profilalkotás során gyűjtött adattípusok csoportosítását az 1. táblázat részletezi.

Fő kategória	Alkategória	Adattípus	Példák
Elsődleges adatokp	Felhasználó által megadott (aktív)	Regisztrációs és személyes adatok	név, e-mail, telefonszám, lakcím, életkor
			regisztráció, vásárlás, ügyfélszolgálati kommunikáció
		Közzétett tartalom	hozzászólás, üzenet, blogbejegyzés, kép-, video-, hangfelvétel, chatbot prompt
	Automatikusan gyűjtött (passzív)	Aktivitással kapcsolatos adatok	böngészési előzmények, keresések, vásárlási, applikációhasználati mintázatok, interakciók
		Technikai és eszközadatok	IP-cím, böngésző, operációs rendszer, eszközazonosítók, nyelvi beállítások, képernyőméret
		Szenzor- és biometrikus adatok	billentyűleütés, kurzormozgás, érintés, járásdinamika
		Helyadatok	GPS, földrajzi hely, mozgásadatok, helyalapú aktivitás
		Külső forrásból származó adatok	nyilvántartások, harmadik felektől vásárolt adatok,
Másodlagos adatok	Következtetett	Pszichológiai jellemzők	személyiségjegyek, hangulat
		Egészségügyi állapot	fizikai vagy mentális állapotra utaló következtetések
		Gazdasági helyzet	jövedelem, hitelképesség
		Demográfiai és társadalmi jellemzők	vallás, ideológia, politikai nézetek
		Preferenciák és érdeklődés	termékpreferenciák, érdeklődési kör
		Viselkedési mintázatok	szokások, rutinok
		Prediktív adatok	döntések, jövőbeli viselkedés előrejelzése

1. táblázat: A felhasználói profilok adatösszetétele, saját szerkesztés

A felhasználói profilalkotás társadalmi kockázatai

Az MI eszközök legújabb változatait övező jelentősebb biztonsági kihívások közé tartozik a félrevezető információk széleskörű vagy célzott terjesztése, a személyes adatok védelmének nehezebbé válása és a tömeges megfigyelés lehetősége. Mindezek a felhaszná-

lói adatok elemzésével nyert átfogó kép segítségével még célzottabbá, pontosabbá, személyre szabottabbá tehetők. Az Anthropic AI fejlesztő vállalat és a Pentagon közt kibontakozó helyzet kapcsán egy 2026.03.06-án közölt videointerjúban [14] Dean Ball a Trump adminisztráció korábbi vezető MI szakpolitikai tanácsadója kifejtette, hogy jogi szempontból a felhasználók eszközeinek kormányzati szervek által történő közvetlen megfigyelése jogellenes cselekedet, ugyanakkor a harmadik felektől vásárolt adatkészletek elemzése nem feltétlenül számít megfigyelési tevékenységnek a jelenlegi USA-beli jogszabályi környezetben.

A technológia emellett megkönnyíti a deepfake tartalmak gyorsabb és meggyőzőbb előállítását, valamint az MI generált tartalmakhoz szükséges bemeneti információk könnyen szennyezhetők (data poisoning), így az MI eszközök, kiemelten a chatbotok a különböző promptokra torzított információt generálhatnak, amely befolyásolhat akár választásokat, vagy aláásható az emberek azon képességét, hogy megbízzanak bármilyen információban, potenciálisan destabilizálva a társadalmakat. [15] Több kutatás született az AI eszközök, chatbotok téves információterjesztéséről, melyet jól szemléltet a Nature 2026. április 07-i cikkében közölt 2024-es kutatás, mely során a Göteborgi egyetem kutatói megalkottak egy fiktív betegséget, hogy teszteljék az MI chatbotokat. A fiktív kórképet leíró információkat első körben egy blogbejegyzésben, majd 2 tudományos publikációban tették közzé. A „csapda cikkek" számos árulkodó jelet tartalmaztak, emellett konkrétan közölték is, hogy „ez az egész tanulmány kitalált". Ennek ellenére a cikkek közlése után, az információ elkezdett megjelenni a leggyakrabban használt LLM chatbotok kimenetében. 2024. április 13-án a Microsoft Bing Copilotja, valamint a Google Geminije, majd 2024. április 27-én a Perplexity AI, majd később a hónap folyamán az OpenAI ChatGPT-je valódinak jelezte a kitalált kórképet a felhasználók felé és tanácsolta nekik, hogy forduljanak orvoshoz. Ezen az ártatlannak tűnő figyelemfelhívó kísérleten túlmutatva az utóbbi években számtalan cikk és kutatás született arról, hogy az MI chat applikációk képesek befolyásolni a felhasználóik politikai nézeteit, valamint hogy mely politikai jelöltekre szavazzanak. Egy a Nature-ben 2025. december 04-én publikált kutatás résztvevőit arra kérték, hogy beszélgessenek olyan nyelvi modellel melyet a kutatók a 2024-es amerikai, a 2025-ös kanadai és a 2025-ös lengyel választások kontextusában különböző jelöltjeinek támogatására tanítottak be. A beszélgetés közvetlen eredményeként 1,52 és 10% közötti volt a választók véleményének változása. [16] Egy másik, a Science folyóiratban publikált kutatás 77 000 brit résztvevő véleményváltozásait vizsgálta, akik 700 különböző politikai vonatkozású kérdésben léptek interakcióba az MI chatbotokkal. A legoptimálisabb modell a résztvevők hozzávetőleg 25%-ának véleményét képes volt megváltoztatni a vizsgált politikai kérdésekben. [17] Ezek a véleménybefolyásolásra irányuló törekvések a dinamikusan változó felhasználói profilok következtetett adataival kombinálva magukban hordozzák a felhasználóra szabott véleménybuborékok és célzott manipuláció vagy mentális állapot befolyásolásának kockázatát.

ADATVÉDELMI KIHÍVÁSOK

A felhasználói profilokra vonatkozó főbb szabályzási kísérletek

A különböző országok különböző megközelítést alkalmaznak a személyes adatok védelmére és a mesterséges intelligencia alkalmazására vonatkozóan. Az Egyesült Álla-

mok, mint az egyik „MI nagyhatalom” a technológia szabályozása tekintetében decentralizált, iparág ösztönző megközelítést részesít előnyben, amely a fejlesztés ösztönzésére összpontosít az átfogó szövetségi korlátozások helyett. [18] Kína hasonlóan ösztönzi a fejlődést, viszont konkrét tiltásokat és irányelveket fogalmaz meg például az MI generált tartalmak jelölésére, vagy az MI modellek tanításához használt bemeneti adatoknál alkalmazandó elővigyázatosságra vonatkozóan. [19] Az Európai Unió ezzel szemben nagyobb hangsúlyt fektet a személyiségi jogi, etikai, versenyegyenlőséget támogató mesterséges intelligencia szabályozásra, valamint konkrét tiltásokat fogalmaz meg.

Az Európai Unió területén belül a legmeghatározóbb adatvédelmi és MI vonatkozású rendelkezések az EU 2016/679 rendelete (továbbiakban GDPR) [20] és az EU 2024/1689 rendelete (továbbiakban MI rendelet) [21]. A felhasználó profil, mint fogalom megjelenik továbbá az EU 2022/2065 rendeletben (továbbiakban: Digitális szolgáltatásokról szóló rendelet) [22], valamint az EU 2023/2854 rendeletében (továbbiakban: Adatrendelet) [23]. Azonban az MI rendelet, az Adatrendelet és a Digitális szolgáltatásokról szóló rendelet is a GDPR 4. cikk 4. pont szerinti definícióra hivatkozik, mely szerint a profilalkotás a „*személyes adatok automatizált kezelésének bármely olyan formája, amelynek során a személyes adatokat valamely természetes személyhez fűződő bizonyos személyes jellemzők értékelésére, különösen a munkahelyi teljesítményhez, gazdasági helyzethez, egészségi állapothoz, személyes preferenciákhoz, érdeklődéshez, megbízhatósághoz, viselkedéshez, tartózkodási helyhez vagy mozgáshoz kapcsolódó jellemzők elemzésére vagy előrejelzésére használják*”. Ebben az értelmezésben a profilalkotás fogalmába a gyűjtött adatok személyazonossággal való egyértelmű összekapcsolása tartozik, különös tekintettel, ha az így gyűjtött adott személyhez köthető adatok, vagy az azokból levonható következtetések adott személy megítélésére hatással lehetnek, ezek miatt negatív diszkrimináció, faji, világnézeti, egyéb orientációra vonatkozó hátrányos megkülönböztetés érheti. A GDPR 22. cikke szabályozza a személyazonosságához köthető profilalkotáson alapuló automatizált döntéshozatalt is (például hitelkérelem elutasítása, dinamikus árképzés, automatikus HR szűrés vagy ügyfélkizárás). Emellett fontosabb profilalkotásra vonatkozó elemei a 13–14. cikkben definiált tájékoztatási kötelezettség, a 21. cikkben kifejtett 4. cikk értelmezése szerinti profilalkotás elleni tiltakozási jog, és a 35. cikk által megfogalmazott adatvédelmi hatásvizsgálat alkalmazása.

Magyar jogszabályi környezetben a 2011. évi CXII. törvényben jelenik meg a profilalkotás definíciója, szintén a GDPR-beli megfogalmazást alkalmazva. Szintén kitér az adatkezelés alanyával szembeni tájékoztatási kötelezettségre (17§ (2)) akkor is, ha az adatkezelő harmadik országbeli (25/E.§). [24] A 17/HU WP251rev.01 NAIH iránymutatása közérthetően összefoglalja a profilalkotás három elemét: „*valamilyen formájú automatizált kezelésnek kell lennie; személyes adatok tekintetében kell végezni; és a profilalkotás célja egy természetes személy személyes jellemzőinek értékelése*.” [25]

Az MI rendeletben megjelenik a biometrikus és viselkedési adatok kezelése, az érzelemfelismerés, valamint ezek és egyéb természetes személyekkel összefüggésbe hozható inputok alapján következtetések levonása is. A rendelet ezeket is első sorban személyiségi jogi szempontból vizsgálja, kiemelten azokra a felhasználási területekre, ahol kiegyenlítetlen hatalmi viszonyok állhatnak fenn és az adatkezelés alanyára az MI rendszer által levont következtetések negatív következménnyel járhatnak (például munkahely, oktatási, egészségügyi intézmények, igazságszolgáltatás bizonyos aspektusai).

Marketingcélú profilalkotás esetén a korlátozások nem egyértelműek

A marketingcélú profilalkotás jelenleg nem rendelkezik egységes, általánosan elfogadott definícióval. Ez a fajta profilalkotás általában nem természetes személyként vizsgálja a felhasználókat, személyazonosságuk nem kerül explicit módon azonosításra. Ennek ellenére a teljes anonimizálás meglehetősen ritka a gyakorlatban, emellett anyagi érdek fűződik a fogyasztói preferenciák lehető legpontosabb feltérképezéséhez. A vállalatok adatkezelés során többnyire egyedi azonosítót (például sütiazonosító vagy eszközazonosító) alkalmaznak. Így a felhasználói paraméterek és interakció továbbra is nyomon követhető tényleges személyazonosítás nélkül. Ugyanakkor az alkalmazáshasználati adatkészletek kinyerése, vagy megosztása továbbra is jelentős adatvédelmi kockázatot jelent. Egy a Helsinki egyetem kutatói által 2022-ben végzett kutatás szerint számos tanulmány kimutatta, hogy a felhasználók azonosíthatók vagy újraazonosíthatók az anonimizált adatkészletekből az alkalmazáshasználati szokásaik alapján. Az elemzett kutatások alapján egy 46 726 résztvevőt magába foglaló vizsgálat során az akkori 500 legnépszerűbb alkalmazás használata által a felhasználók 99,67%-ánál egyedi alkalmazás-aláírást lehetett létrehozni. Egy nagyobb, 1,37 millió kínai felhasználóból álló adatkészletet elemzése alapján mindössze 4 alkalmazás használata által a felhasználók 88%-át lehetséges egyedileg azonosítani. [26]

Sötét mintázatok alkalmazása a felhasználók tájékoztatásában

A sütik elfogadására vonatkozó bannerek és az adatvédelmi irányelvek kontextusában a sötét mintázatok olyan felhasználói felület-kialakítások vagy kommunikációs gyakorlatok, amelyeket szándékosan úgy alakítottak ki, hogy befolyásolják, nyomást gyakoroljanak, összezavarják vagy manipulálják a felhasználókat, hogy hozzájáruljanak az olyan adatgyűjtési, -követési vagy -megosztási gyakorlatokhoz, amelyeket megfelelő tájékoztatás és egyértelmű választási lehetőségek esetén elutasítanának. Ha feltételezzük, hogy a felhasználói adatok többségének kezelése explicit, önkéntes hozzájárulásuk alapján történik, akkor is figyelembe kell venni az alábbi döntéseiket befolyásoló tényezőket.

Az EU jogszabályi környezete egyértelműen definiálja a felhasználók tájékoztatására vonatkozó paramétereket, a nem megfelelő tájékoztatást komoly bírságokkal szankcionálja. Azonban a gyakorlatban a tájékoztatás minősége és az adatkezelés jogszerűsége gyakran elmarad az elvárásoktól. Egy 2012-es felmérés szerint egy felhasználónak körülbelül 76 napba telne elolvasni azon adatkezelési tájékoztatókat, melyekkel egy év alatt találkozik. [27] Egy 50000 adatkezelési tájékoztatót vizsgáló 2021-es elemzés szerint egy adatkezelési tájékoztató hossza 4000 szó terjedelmű, emellett az átlagos felhasználók számára gyakran nehezen értelmezhető jogi nyelvezettel íródnak. [28] Egy 2024-es felmérés szerint a vizsgált felhasználók körülbelül 0,5%-a nyitotta meg az adatkezelési tájékoztatókat. A tanulmányban vizsgált dokumentumok már átlagosan 7400 szó hosszúságúak voltak. [29]

A GDPR rendelkezése szerint hozzájárulásnak tájékoztatáson alapulónak, konkrétnak és önkéntesnek kell lennie. Ezzel szemben számos weboldal nem ad választási lehetőséget sem, kizárólag egy felugró ablakban tájékoztat, hogy az adott oldal sütiket használ, kezeli a felhasználó adatait. A sütik elfogadására vonatkozó bannerek gyakran alkalmaznak GDPR rendelkezéseket sértő módszereket a grafikus kialakítás, szövegezés, vagy választási lehetőségek láthatósága terén. A felhasználó kognitív kifáradására, érzéketlenedésére alapozva túlterhelő mennyiségű egyesével kiválasztandó kategóriára bontják a hozzájárulást,

elrejtik a visszautasítás opciót, kiemelik a minden süti elfogadására irányuló lehetőséget, előre bejelölik az összes kezelni kívánt sütikategóriát, vagy félreértelmezhető, esetleg megtévesztő módon ábrázolják az elfogadást és elutasítást jelző gombokat. A sütik elutasítását indokolatlanul hosszú, következetlen vagy nehezen átlátható folyamatok nehezítik, miközben az adatkezelés elfogadása egyszerű és gyors marad. Ezzel párhuzamosan a rendszerek gyakran alkalmaznak túlzott egyszerűsítést, személyre szabást és célzott javaslatokat, amelyek a kívánt döntési útvonalat intuitívabbnak és relevánsabbnak tüntetik fel. Ezek mellett a felhasználói profilalkotás segítségével felületek folyamatosan adaptálódnak a változó felhasználói szokásokhoz a kívánt adatkezelési eredmények elérése érdekében. [30] Egyre gyakrabban megjelenik a sütik elutasítási lehetőségének fizetési fal mögé helyezése is, ahol a felhasználó választhat, hogy előfizet, vagy beleegyezik az adatkezelésbe a „jobb felhasználói élmény" érdekében.

A szabályozás gyakorlati korlátai

Olyan non-profit szervezetek, mint a NYOB a sötét mintázatok alkalmazása kapcsán közel 10000 európai weboldalt vizsgált felül nem megfelelő gyakorlataik kapcsán, mely eredményeként több mint 500 vállalat kapott írásbeli figyelmeztetést 2021 tavaszáig. A jogsértések 42%-át 30 napon belül remediálták, viszont a vizsgált vállalatok 82%-ánál alkalmazott gyakorlatok továbbra is sértik a GDPR-t. Ennek megfelelően további 422 panasz került benyújtásra 10 adatvédelmi hatósághoz. [31] A Meta részére az utóbbi években több jelentős adatvédelmi vonatkozású bírság került kiszabásra, melyek közül a legismertebb a 2023 májusi 1,2 milliárd euró összegű bírságot eredményező adatátviteli szabálysértés, melyet a felhasználói adatok az Európia Unióból az USA-ba továbbítása eredményezett. [32] Majd további nagy nyilvánossággal járó bírságokat kaptak felhasználókat célzó webes adatkinyerés miatt 2022-ben, a felhasználói jelszavak egyszerű szöveg alapú tárolásáért 2024 szeptemberében, valamint egyéb nem megfelelő jelszókezelési gyakorlatok miatt 2024 decemberében. Ugyan a 2023-as eset korábban példátlan mértékű bírságot eredményezett, számításba kell venni, hogy a vállalat teljes piaci értékét a 2023 májusában több mint 520 milliárd, jelenleg 2026 májusában pedig 1,5-1,6 trillió dollárra becsülik. [33] A megfelelő jogi és technológiai kontrollok implementálásának és betartatásának legjelentősebb akadályai a fejlődés rendkívül gyors üteme, valamint az egyre nagyobb számú digitális szolgáltató egyidejű jelenléte és az adatvédelmi incidensek kivizsgálási ideje, valamint a bírság és remediálás megállapításához vezető idő hossza. Emellett a kontrollok érvényesítése gyakran gazdasági vagy politikai érdekbe ütközik. Jól szemlélteti ezen kezdeményezések akadályait az MI technológiákról szóló kommunikáció ellentmondásos hatása is. Hetente jelennek meg különböző médiumokban a keresőoptimalizált, hangzatos főcímek az emberiséget elpusztító mesterséges intelligenciáról szóló elméletekről és találgatásokról. Az ilyen típusú kommunikáció viszont paradox módon erősíti a technológiai óriásvállalatok pozícióját, és akadályozza a mesterséges intelligencia által jelenleg okozott negatív társadalmi hatások hatékony szabályozását, ahogy a *Nature* 2023 júniusában megjelent cikkében összegzett szakértői vélemények is alátámasztják [34]. Ezen értelmezés szerint a mesterséges intelligencia, „tökéletes fegyverként" való ábrázolása táplálja a nemzetek közötti fejlesztési versenyt az előnyszerzés és a lehető leghatékonyabb MI eszközök saját irányításuk

alá vonása érdekében. Ezáltal ösztönzi a beruházásokat és akadályozza az iparág szabályozását célzó kezdeményezéseket, valamint lehetővé teszi, hogy nagyvállalati vezetők szűk csoportjai befolyásolják azokat.

ÖSSZEFOGLALÁS

A profilalkotásnak különböző definíciói léteznek ágazattól, felhasználási módtól függően. A felhasználókról gyűjtött adatok elemzésével létrehozott profilok használhatók többek között kibervédelmi anomáliadetektálásra, szervezeti munkafolyamat optimalizálása, vagy ügyfélinterakciók elemzésére, termékfejlesztés és üzleti stratégiai döntések elősegítése céljából. A profilalkotás során gyűjtött hatalmas mennyiségű adat önmagában is jelentős értéket képvisel mind gazdasági, mind biztonsági szempontból. Ezen felül az utóbbi években a digitalizáció terjedése, és a mesterséges intelligencia forradalma új dimenziót nyitott a felhasználói adatok feldolgozásában, mely hatására az eddig emberi léptékkel belátható időn belül feldolgozhatatlan mennyiségű adatból struktúrált, akár valós időben változó, nagy pontosságú kép alakítható ki a vizsgált felhasználókról, így akár jövőbeli döntéseik is előrejelezhetővé válhatnak. A felhasználói profilalkotás fejlődése nyilvánvaló előnyei mellett számos új biztonsági kihívást magával hozott, mivel a marketingcélú felhasználás mellett akár kifinomult kibertámadásokhoz, vagy politikai véleménybefolyásoláshoz is felhasználható. A kockázatok mitigálása érdekében a különböző országok jogalkotói megkísérelték szabályozni a felhasználókról gyűjthető adatok felhasználási és kezelési módjait, igyekezve lépést tartani a fejlődéssel. A szabályozói kontrollkörnyezet kialakításában azonban jelentős kihívást okoz a gazdasági érdekek és a felhasználók jogainak érvényesítése közötti érdekellentét. Ennek eredményeként számos szabályozói szürke zóna alakult ki a felhasználói profilalkotás szabályozása terén, továbbá a gyors ütemű technológiai fejlődés gyakran meghaladja a jogalkotók alkalmazkodásának ütemét. A Európai Unió mesterséges intelligencia alapú felhasználói profilalkotásra vonatkozó szabályozási környezete jelenleg nem rendelkeznek egyértelműen a marketikg célból létrehozott felhasználói profilok adattartalmáról és felhasználásuk korlátozásáról. A magas bírságok ellenére a felhasználói adatok kezelésére vonatkoztató tájékoztatás, adatkezelési gyakorlatok gyakran nem kellőképpen transzparensek, valamint a szabálytalan gyakorlat beazonosításától annak szankcionálásáig és részleges vagy teljes mitigálásig akár évek is eltelhetnek. Emellett a felhasználói profilkészítésben rejlő anyagi előnyök messze túlmutatnak a büntetések mértékén. Ezért szükséges a felhasználók megfelelő edukációja online aktivitásuk lehetséges következményeit, digitális lábnyomuk összetételét, adatvédelmi jogaik érvényesítési lehetőségeit illetően, és a manipulációs technikák felismerése terén. Valamint a vállalatok és nemzetek vezetőinek nagyobb hangsúlyt kell helyezniük az állampolgárok digitális biztonságtudatossági oktatására, a digitális lábnyom adatösszetételére és a kockázatarányos felkészülés érdekében számításba kell venniük azokat a szcenáriókat, amikor ezen adatok felhasználása ellenséges vagy manipulatív szándékkal történik.

FELHASZNÁLT IRODALOM

[1] Mordor Intelligence, “User Activity Monitoring Market - Growth, Trends, COVID-19 Impact, and Forecasts,” Mordor Intelligence, Elérés: https://www.mordorintelligence.com/industry-reports/user-activity-monitoring-market

[2] Strategic Market Research, "Behavior Analytics Market," Strategic Market Research, 2025. Okt. Elérés: https://www.strategicmarketresearch.com/market-report/behavior-analytics-market
[3] Market Growth Reports, "Customer Analytics Market Report," Market Growth Reports, 2026. Jan. Elérés: https://www.marketgrowthreports.com/market-reports/customer-analytics-market-114920
[4] Intellect Markets, "Customer Behavior Analytics Market," Intellect Markets, Elérés: https://intellectmarkets.com/report/customer-behavior-analytics-market
[5] J. Amankwah-Amoah, Z. Khan, G. Wood, and G. Knight, "COVID-19 and Digitalization: The Great Acceleration," Journal of Business Research, 2021. Nov. Elérés: https://www.sciencedirect.com/science/article/pii/S0148296321005725?via%3Dihub
[6] "How Ernest Dichter Brought Psychology to Business," *Psychology Today*, 2022. Ápr. Elérés: https://www.psychologytoday.com/us/blog/psychology-yesterday/202204/how-ernest-dichter-brought-psychology-business
[7] S. C. Matz, M. Kosinski, G. Nave, and D. J. Stillwell, "Psychological targeting as an effective approach to digital mass persuasion," *Proceedings of the National Academy of Sciences*, 2017. Nov. https://www.pnas.org/doi/10.1073/pnas.1710966114
[8] "The Cambridge Analytica scandal and what it teaches us," *University of Greater Manchester Blog*. 2021. Ápr. 19, Elérés: https://greatermanchester.ac.uk/blogs/the-cambridge-analytica-scandal-and-what-it-teaches-us
[9] A. Alifar, "Exposed: Google is indexing private AI conversations — here's what you should know," *DEV Community*, 2025. Júl. Elérés: https://dev.to/alifar/exposed-google-is-indexing-private-ai-conversations-heres-what-you-should-know-37m5
[10] "The Old Rules Are Dead," *Quantable*. Elérés: https://www.quantable.com/ai/the-old-rules-are-dead/
[11] V. Kumar and M. Lata, "AI chatbots: security and privacy challenges," *International Journal of Electronic Security and Digital Forensics*, vol. 17, pp. 776–797, 2025. Jan, Elérés: https://www.researchgate.net/publication/387605688_ai_chatbots_security_and_privacy_challenges
[12] F. Bulut Kartal and E. Yildirim, "AI profiling poses growing threat to privacy and national security," *Anadolu Agency*, 2025. Júl. 10, Elérés: https://www.aa.com.tr/en/artificial-intelligence/ai-profiling-poses-growing-threat-to-privacy-and-national-security/3627228
[13] C. L. Miltgen, A. Popovič, and T. Oliveira, "Determinants of end-user acceptance of biometrics: Integrating the 'Big 3' of technology acceptance with privacy context," *Decision Support Systems*, vol. 56, no. 1, pp. 103–114, 2013. Dec. Elérés: https://www.sciencedirect.com/science/article/abs/pii/S0167923613001267.
[14] Ezra Klein, Dean Ball, „*Why the Pentagon Wants to Destroy Anthropic*" 2026. Márc. 6. Elérés: https://www.youtube.com/watch?v=xc97F2CFBOY
[15] D. Matthews, "Scientists invented a fake disease. AI told people it was real," Nature, 2026. Ápr. 7, Elérés: https://www.nature.com/articles/d41586-026-01100-y
[16] H. Lin, G. Czarnek, B. Lewis, J. P. White, A. J. Berinsky, T. Costello, G. Pennycook, and D. G. Rand, "Persuading voters using human–artificial intelligence dialogues," Nature, 2025. Dec. 4, Elérés: https://www.nature.com/articles/s41586-025-09771-9

[17] M. V. Gómez, “Programs like ChatGPT can change the opinion of one in four voters,” El País, 2025. Dec. 4, Elérés: https://english.elpais.com/technology/2025-12-04/programs-like-chatgpt-can-change-the-opinion-of-one-in-four-voters.html
[18] The White House, “National Policy Framework for Artificial Intelligence: Legislative Recommendations,” 2026. Mar. Elérés: https://www.whitehouse.gov/wp-content/uploads/2026/03/03.20.26-national-policy-framework-for-artificial-intelligence-legislative-recommendations.pdf
[19] CMS Expert Guides, “AI laws and regulation in China.” Elérés: https://cms.law/en/int/expert-guides/ai-regulation-scanner/china
[25] National Authority for Data Protection and Freedom of Information (NAIH), “Iránymutatás az automatizált döntéshozatallal és a profilalkotással kapcsolatban a 2016/679 rendelet alkalmazásához,” Elérés: https://www.naih.hu/files/wp251rev01_hu.pdf
[26] T. Li, “Smartphone App Usage Analysis: Datasets, Methods, and Applications,” *IEEE*, 2022. Elérés: https://helda.helsinki.fi/server/api/core/bitstreams/54d45a59-3295-4c63-a28f-1e5ff33ec903/content
[27] A. C. Madrigal, “Reading the Privacy Policies You Encounter in a Year Would Take 76 Work Days,” *The Atlantic*, 2012. Mar. 1, Elérés: https://www.theatlantic.com/technology/archive/2012/03/reading-the-privacy-policies-you-encounter-in-a-year-would-take-76-work-days/253851/
[28] De Montfort University Leicester, “Study shows privacy policies are longer and harder to understand in 2021,” 2022. Febr. Elérés: https://www.dmu.ac.uk/about-dmu/news/2022/february/study-shows-privacy-policies-are-longer-and-harder-to-understand-in-2021.aspx
[29] Linklaters, “Who reads privacy notices? And why do we have them?” *Digilinks Blog*, 2024. Szept. 26, Elérés: https://www.linklaters.com/insights/blogs/digilinks/2024/september/uk---who-reads-privacy-notices-and-why-do-we-have-them
[30] A. Mathur, M. Kshirsagar, and J. Mayer, “Dark design patterns: An end-user perspective,” *Human Technology*, vol. 16, no. 2, pp. 170–199, 2020. Aug. Elérés: https://www.researchgate.net/publication/346663816_dark_design_patterns_an_end-user_perspective
[31] noyb – European Center for Digital Rights, “noyb files 422 formal GDPR complaints on nerve-wrecking ‘Cookie Banners’,” 2021. Aug. 10, Elérés: https://noyb.eu/en/noyb-files-422-formal-gdpr-complaints-nerve-wrecking-cookie-banners
[32] European Data Protection Board (EDPB), “1.2 billion euro fine for Facebook as a result of EDPB binding decision,” 2023. Máj. 22, Elérés: https://www.edpb.europa.eu/news/news/2023/12-billion-euro-fine-facebook-result-edpb-binding-decision_en
[33] CompaniesMarketCap, “Market capitalization of Meta Platforms (Facebook) (META).” Elérés: https://companiesmarketcap.com/meta-platforms/marketcap/#google_vignette
[34] *Nature*, “Stop talking about tomorrow’s AI doomsday when AI poses risks today,” 2023. Jún. 27, Elérés: https://www.nature.com/articles/d41586-023-02094-7

JOGSZABÁLYOK

[20] Az Európai Parlament és a Tanács (EU) 2016/679 rendelete (általános adatvédelmi rendelet – GDPR), *Official Journal of the European Union*, 2016. Ápr. 27, Elérés: https://eur-lex.europa.eu/legal-content/HU/TXT/?uri=CELEX:32016R0679

[21] Az Európai Parlament és a Tanács (EU) 2024/1689 rendelete a mesterséges intelligenciára vonatkozó harmonizált szabályokról (Mesterséges Intelligencia Rendelet), *Official Journal of the European Union*, 2024. Jún. 13, Elérés: https://eur-lex.europa.eu/legal-content/HU/TXT/?uri=CELEX:32024R1689

[22] Az Európai Parlament és a Tanács (EU) 2022/2065 rendelete a digitális szolgáltatások egységes piacáról (digitális szolgáltatásokról szóló rendelet – DSA),” *Official Journal of the European Union*, 2022. Okt. 19, Elérés: https://eur-lex.europa.eu/eli/reg/2022/2065/oj/hun

[23] Az Európai Parlament és a Tanács (EU) 2023/2854 rendelete az adatokhoz való méltányos hozzáférésről és felhasználásról (adatmegosztási rendelet – Data Act), *Official Journal of the European Union*, 2023. Dec. 13, Elérés: https://eur-lex.europa.eu/eli/reg/2023/2854/oj?locale=hu

[24] Magyarország Országgyűlése, 2011. évi CXII. törvény az információs önrendelkezési jogról és az információszabadságról Elérés: https://net.jogtar.hu/jogszabaly?docid=a1100112.tv