JOGI FÓRUM PUBLIKÁCIÓ

www.jogiforum.hu

Az adatkezelésről való tájékoztatás technológiai környezetben, különös tekintettel az Egyesült Államok szabályozására

Szerző:

Dr. Necz Dániel

Kézirat lezárva: 2022.08.31

Az Innovációs és Technológiai Minisztérium ÚNKP-21-3 kódszámú Új Nemzeti Kiválóság Programjának a Nemzeti Kutatási, Fejlesztési és Innovációs Alapból finanszírozott szakmai támogatásával készült.

I. Bevezetés

Az adatkezelésről való tájékoztatás az adatvédelmi szabályozás egyik sarokpontjának tekinthető, amely megteremti az adatkezelés transzparens jellegét, és egyben biztosítja az érintett adatvédelmi jogainak gyakorlását. Ennek segítségével ugyanis az érintett átláthatja az adatkezelési műveleteket, és tisztában lehet azzal, hogy jogainak gyakorlása hogyan hathat az adatkezelésre, az érintett jogaira és szabadságaira, valamint hogyan változtathatja meg az érintett helyzetét.

A tájékoztatás, mint a jogszerű és etikus adatkezelés egyik garanciája az adatkezelés valamennyi típusa esetén kulcsfontosságúnak tekinthető, különös jelentőséggel bír azonban a technológiai környezetben végzett adatkezelések esetén, ahol az érintett információs jogai és lehetőségei a gyakorlatban még inkább korlátozottak. Így egy kórházban ápolt beteg eleve kevesebb lehetőséggel bír egészségügyi adatai kezelésének áttekintése, az abba való esetleges beleszólás kapcsán, amennyiben azonban az egészségügyi szolgáltató ezen adatokat kutatási célból elemzi vagy az egészségügyi szolgáltatások erősítése céljából ápoló robotokat alkalmaz, úgy a beteg lehetőségei még inkább korlátozottabbak személyes adatai kezelésének, valamint azok jelentőségének felfogására, így az adatkezelőként eljáró egészségügyi intézménytől elvárható, hogy tartózkodjon ezen „információs erőfölénnyel” való visszaéléstől, az érintett beteg adatait elsősorban az ő érdekében használja fel, valamint egyértelmű tájékoztatást nyújtson a személyes adatok kezeléséről, annak jelentőségéről.

Természetesen az adatkezelésről való tájékoztatás problematikáját az egyes országok joga, valamint bírósági és hatósági gyakorlata eltérő módon közelíti meg, különösen ideértve a technológiai környezetben végzett adatkezelési műveleteket, így az e körben tett észrevételek csak ezen eltérésekre, a különböző jogi kultúrák szemléletével összhangban foghatnak helyet. Mindemellett az egyes szabályozási törekvések kapcsán álláspontunk szerint különös hangsúlyt érdemelnek az Egyesült Államok szabályozási törekvései, kiemelten a mesterséges intelligencia és az adatvédelem területén, ugyanakkor nem hagyhatók figyelmen kívül az elmúlt évek európai uniós jogi fejleményei sem.

Az Innovációs és Technológiai Minisztérium ÚNKP-21-3 kódszámú Új Nemzeti Kiválóság Programjának a Nemzeti Kutatási, Fejlesztési és Innovációs Alapból finanszírozott szakmai támogatásával készült.

A fentiekre tekintettel a jelen tanulmány célja az adatkezelésről való tájékoztatás problematikájának bemutatása technológiai környezetben, különös tekintettel az Amerikai Egyesült Államok szabályozására, ideértve mind a szövetségi, mind a tagállami szabályozást, valamint az egyes hatóságok megközelítését, és a releváns bírósági és hatósági gyakorlatot. Ugyanakkor sor kerül az amerikaival szembenálló európai megközelítés, illetve az Európai Unió szabályozásának bemutatására is, tekintettel arra, hogy különösen ennek révén alkotható teljes kép az eltérő szabályozási megközelítésekről, valamint szempontokról.

A tanulmány az amerikai és a sok szempontból ellenpólusként értelmezhető európai szabályozás bemutatásán túl különös gondot fordít az adatkezelésről való tájékoztatás problémakörének feltárására az egyes technológiai vívmányok tükrében is, figyelemmel arra, hogy az adott technológiai környezet és annak sajátos aspektusainak bemutatása hiányában nem alkotható megfelelő kép az átláthatóság gyakorlati követelményéről. Erre tekintettel a jelen tanulmány célja az amerikai szabályozás és az annak ellenpólusát képező szempontok bemutatásán túl különösen a mesterséges intelligencia általi adatkezelés, valamint az egyéb technológiai megoldások átláthatóságával kapcsolatos szabályozói, valamint szakirodalmi megközelítések, releváns bírói, illetve hatósági gyakorlat feltárása és bemutatása.

Az Innovációs és Technológiai Minisztérium ÚNKP-21-3 kódszámú Új Nemzeti Kiválóság Programjának a Nemzeti Kutatási, Fejlesztési és Innovációs Alapból finanszírozott szakmai támogatásával készült.

II. Az adatkezelésről való tájékoztatás az Amerikai Egyesült Államok szabályozásának tükrében

1. A szövetségi szabályozás

A szövetségi szabályozás elsősorban az olyan területek szabályozására helyezi a fókuszt, ahol az érintettek jellemzően gyengébb helyzetben vannak az adatkezelővel szemben, így a személyes adataik kezelésével kapcsolatos transzparencia megkövetelése segítséget nyújt a számukra az esetleges jogsértő adatkezeléssel szembeni fellépés kapcsán, egyben számos esetben korlátot is szab a személyes adatokkal való visszaélésnek. Ezen területek közé tartozik például az egészségügyi célú vagy a pénzügyi szolgáltatók általi adatkezelés, emellett azonban a szövetségi jog kiemelt módon védi a gyermekek adatainak interneten keresztül történő gyűjtését és felhasználását, amellyel kapcsolatosan átláthatósági követelményeket is rögzít.

A fentiekre tekintettel szövetségi szabályozás védi a gyermekek adatainak kezelését az online környezetben. Így a Children's Online Privacy Protection Rule (COPPA) elnevezésű törvény[1] tiltja a 13. életév alatti gyermekek adatainak tisztességtelen, illetve visszaélésszerű gyűjtését, valamint felhasználását az interneten. Ezenkívül egyéb kötelezettségeket is előír a törvény weboldalak üzemeltetői, valamint online szolgáltatások nyújtói számára, ideértve különösen az érintettek nyilvános tájékoztatását, az üzemeltető, illetve szolgáltató kapcsolattartási adatainak feltüntetését, valamint bizonyos kivételekkel szülői hozzájárulás bekérését.

[1] https://www.ecfr.gov/current/title-16/chapter-I/subchapter-C/part-312 [2022.08.26.]

Az Innovációs és Technológiai Minisztérium ÚNKP-21-3 kódszámú Új Nemzeti Kiválóság Programjának a Nemzeti Kutatási, Fejlesztési és Innovációs Alapból finanszírozott szakmai támogatásával készült.

2. A tagállami szabályozás

A személyes adatok technológiai környezetben való kezelése kapcsán számos esetben a tagállami jog is tartalmaz előírásokat, amelyek nagyobb fokú transzparenciát várnak el egyes szolgáltatások nyújtóitól vagy egyes kiemelt fontosságú feladatot ellátó személyektől vagy szervezetektől (például: egészségügyi intézmények vagy pénzügyi szolgáltatók általi adatkezelés).

Emellett kiemelendő, miszerint a tagállami adatvédelmi szabályozások kulcspontját számos esetben a fogyasztók adatainak kezelése képezi, kiemelten ideértve a technológiai környezetben való nagy számú személyes adat kezelését. A jelen tanulmány megjelenéséig Kalifornia, Colorado, Connecticut, Virginia és Utah államok rendelkeznek átfogó adatvédelmi jogszabályokkal, amelyek a fentebb írtak szerint számos esetben a fogyasztók adatainak védelmére fókuszálnak.[2] Emellett azonban szinte valamennyi állam rendelkezik olyan jogszabályokkal, amelyek egy-egy szektor vagy tevékenység vonatkozásában rögzítenek adatvédelmi tárgyú rendelkezéseket (például: a személyes adatokról való tájékoztatás megkövetelése a betegek adatainak egészségügyi szolgáltató általi kezelése vagy weboldal működtetése esetén).

A fentiekre jó példának tekinthető a California Consumer Privacy Act (CCPA)[3]. A jogszabály azon vállalkozásokra terjed ki, amelyek Kalifornia államban folytatnak kereskedelmi tevékenységet, valamint az éves bruttó árbevételük a 25 millió dollár összeget meghaladja, legalább 50.000 kaliforniai lakos, háztartás vagy eszköz adatait adják el, veszik meg, vagy részesülnek ilyen adatokban más szervezetektől, és éves árbevételük legalább 50%-át kaliforniai lakosok adatainak eladásából szerzik, így tehát a CCPA hatálya jelentős mértékben a nagy technológiai, valamint az adatelemzés és az online marketing

[2] Taylor Key Lively, US State Privacy Legislation Tracker, 2022.08.11, https://iapp.org/resources/article/us-state-privacy-legislation-tracker/
[3]California Consumer Privacy Act of 2018, https://leginfo.legislature.ca.gov/faces/codes_displayText.xhtml?division=3.&part=4.&lawCode=CIV&title=1.81.5 [2022.08.29]

Az Innovációs és Technológiai Minisztérium ÚNKP-21-3 kódszámú Új Nemzeti Kiválóság Programjának a Nemzeti Kutatási, Fejlesztési és Innovációs Alapból finanszírozott szakmai támogatásával készült.

területén aktív cégekre terjed ki, a kisvállalkozások, illetve az eltérő területeken tevékenységet folytató vállalkozásokra azonban a szabályozás nem vonatkozik.

Hasonlóan az Európai Általános Adatvédelmi Rendelethez (GDPR), a CCPA is számos jogot biztosít az érintetteknek, ideértve – többek között – a tájékoztatáshoz, az adatkezelés korlátozásához (zároláshoz) vagy az adatok törléséhez való jogot. A CCPA értelmében továbbá a vállalkozások nem diszkriminálhatják azon érintetteket, akik a CCPA szerinti jogaikkal élnek, így az érintettek nem hozhatók olyan helyzetbe, hogy kénytelenek legyenek adatvédelmi jogaik gyakorlásától eltekinteni, például az adott vállalkozás kirekesztő kereskedelmi gyakorlata okán. A fentiek kapcsán megemlítendő, hogy Kalifornia állam 2020. novemberében elfogadta a California Privacy Rights and Enforcement Act of 2020 (CPRA) elnevezésű jogszabályt, amely 2023. január 1-én lép hatályba, és kiterjeszti a CCPA hatályát, valamint egyúttal létrehozza az adatvédelmi ügyekkel foglalkozó California Privacy Protection Agency elnevezésű hivatalt.[4]

Hangsúlyozandó azonban, hogy más tagállamok adatvédelmi törvényei jellemzően eltérő vállalkozásokra terjednek ki, valamint több esetben eltérő jogokat biztosítanak az érintettek részére, illetve eltérő kötelezettségeket írnak elő a szabályozás által érintett vállalkozások számára. Így például a Virginia Consumer Data Protection Act azon Virginia-ban tevékenykedő vállalkozásokra terjed ki, amelyek egy adott évben legalább 100.000 fogyasztó adatait kezelik, vagy legalább 25.000 fogyasztó adatait kezelik, és bruttó árbevételük több mint 50%-át személyes adatok eladásából szerzik[5], míg Colorado állam Colorado Privacy Act elnevezésű törvénye azon Colorado-ban tevékenykedő vállalkozásokra terjed ki, amelyek egy naptári évben legalább 100.000 fogyasztó adatait kezelik, vagy bevételt szereznek, illetve árengedményt kapnak személyes adatok eladásából, és legalább 25.000 fogyasztó adatait kezelik.[6] A fentieken túl az érintettek jogai, valamint a vállalkozások kötelezettségei között is bizonyos eltérések tapasztalhatók. Így például Virginia, Colorado és Connecticut államok szabályozása előír adott esetben

[4] IAPP, https://iapp.org/resources/topics/ccpa-and-cpra/ [2022.08.31]
[5] Code of Virginia, Title 59.1, Chapter 53. Consumer Data Protection Act, https://law.lis.virginia.gov/vacode/title59.1/chapter53/section59.1-576/ [2022.08.30]
[6] Colorado Revised Statutes, Part 13. Colorado Privacy Act, https://law.lis.virginia.gov/vacode/title59.1/chapter53/section59.1-576/ [2022.08.30]

Az Innovációs és Technológiai Minisztérium ÚNKP-21-3 kódszámú Új Nemzeti Kiválóság Programjának a Nemzeti Kutatási, Fejlesztési és Innovációs Alapból finanszírozott szakmai támogatásával készült.

kockázatértékelési kötelezettséget az adatkezelők számára, míg Utah állam joga nem.[7] Kiemelendő továbbá, hogy több más államban is benyújtásra kerültek átfogó jellegű adatvédelmi tárgyú jogszabályok tervezetei az elmúlt időszakban, így a közeljövőben még aktívabb szabályozásra lehet számítani az Egyesült Államokban az adatvédelem és a technológiai jog területén.

[7] Taylor Key Lively [2]

Az Innovációs és Technológiai Minisztérium ÚNKP-21-3 kódszámú Új Nemzeti Kiválóság Programjának a Nemzeti Kutatási, Fejlesztési és Innovációs Alapból finanszírozott szakmai támogatásával készült.

III. Az adatkezelésről való tájékoztatás az Európai Unió szabályozásának tükrében

A tájékoztatás a korábban említettek szerint az adatkezelő egyik alapvető kötelezettségének tekinthető, amely átláthatóvá teszi az adatkezelést, egyúttal lehetővé teszi az érintett számára az adatkezelés megismerését, továbbá az érintetti jogok és jogorvoslati lehetőségek hatékony gyakorlását. Mindez következik 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 irányelv hatályon kívül helyezéséről („**GDPR**”)[8] első, jogszerűséggel, tisztességes eljárással és átláthatósággal kapcsolatos alapelvéből[9] is, miszerint a „*természetes személyek számára átláthatónak kell lennie, hogy a rájuk vonatkozó személyes adataikat hogyan gyűjtik, használják fel, azokba hogy tekintenek bele vagy milyen egyéb módon kezelik, valamint azzal összefüggésben, hogy a személyes adatokat milyen mértékben kezelik vagy fogják kezelni*”; az átláthatóság elve megköveteli továbbá, hogy az érintettek részére nyújtott tájékoztatás „*könnyen hozzáférhető és közérthető legyen, valamint hogy azt világosan és egyszerű nyelvezettel fogalmazzák meg.*”[10] Ennek tükrében tehát a különösen technológiai eszközökkel történő adatkezelés átláthatatlan alkalmazása, az érintettek nem megfelelő tájékoztatása a tisztességes adatkezelés követelményét is sértheti.[11]

A fentiekből következően a tájékoztatás nyelvezete az érintetti kör számára minden esetben közérthető kell, hogy legyen. Amennyiben tehát az érintetti kör szakértőkből áll, úgy a tájékoztatás számukra tartalmazhat releváns szakkifejezéseket, míg laikus érintetti kör esetén a túlzottan technológiai, szakmai vagy nehezen érthető kifejezések használata minden esetben kerülendő. Erre tekintettel a Nemzeti Adatvédelmi és Információszabadság egy ügyben megállapította, miszerint az

[8] 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 irányelv hatályon kívül helyezéséről (általános adatvédelmi rendelet), OJ L 119, 4.5.2016, p. 1–88 (BG, ES, CS, DA, DE, ET, EL, EN, FR, GA, HR, IT, LV, LT, HU, MT, NL, PL, PT, RO, SK, SL, FI, SV).
[9] GDPR 5. cikk (1)(a) pontja „*A személyes adatok kezelését jogszerűen és tisztességesen, valamint az érintett számára átlátható módon kell végezni („jogszerűség, tisztességes eljárás és átláthatóság”)*”.
[10] GDPR (39) preambulum-bekezdés.
[11] Péterfalvi Attila, Algoritmusok és adatvédelem: Quo vadis? 179-185. o. In: Török Bernát, Ződi Zsolt (szerk.), A mesterséges intelligencia szabályozási kihívásai, Ludovika Egyetemi Kiadó, Budapest, 2021, 183. o.

Az Innovációs és Technológiai Minisztérium ÚNKP-21-3 kódszámú Új Nemzeti Kiválóság Programjának a Nemzeti Kutatási, Fejlesztési és Innovációs Alapból finanszírozott szakmai támogatásával készült.

„„ügyfélszegmentációs szimuláció elvégzése" adatkezelési cél esetében az érintettek számára egyáltalán nem értelmezhető, hogy mit jelent az „ügyfélszegmentáció", illetve e vonatkozásban milyen tevékenységet jelent a „szimulációk elvégzése". Ezeknek a kifejezéseknek nincs olyan, a hétköznapi életben is bevett jelentése, amely alapján az érintettek azonosítani tudnák, hogy milyen adatkezelést végez a Kötelezett."[12] Amennyiben pedig az érintett fogyatékossága miatt nem érti a tájékoztatást, úgy a szükséges körben gondoskodni kell a részére a tájékoztatás megértésének technikai és egyéb módszereiről (például: az adatvédelmi tájékoztató Braille írással történő közzététele, látássérült érintettek adatainak kezelése esetén).

Hangsúlyozandó, hogy amennyiben az adatkezelés automatizált döntéshozatallal, illetve profilalkotással jár, úgy ennek kapcsán további tájékoztatási kötelezettség terheli az adatkezelőt. Ennek kapcsán profilalkotásnak minősül 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"*[13], míg automatizált döntéshozatalnak tekinthető az olyan automatizált adatkezelésen alapuló döntés, amely az érintettre nézve joghatással jár vagy őt hasonlóképpen jelentős mértékben érinti.[14] Ennek kapcsán „joghatással járónak" tekinthető a döntés, amennyiben például egy szerződés megszüntetéséhez vagy szociális juttatás nyújtásához, vagy ennek elutasításához vezethet, illetve ehhez hasonlóképp jelentős hatással járónak tekinthető a döntés, amennyiben az érintett körülményeit, viselkedését vagy választásait jelentősen befolyásolja, rá nézve hosszan tartó vagy tartós hatással bír, illetve vele szemben diszkriminációhoz vezethet; ennek kapcsán azonban értelemszerűen csak esetről-esetre ítélhető meg, hogy az adott döntés, illetve annak hatásai kellő jelentőséggel bírnak-e. E körbe tartozhat például az érintett hitelminősítésével vagy egészségügyi szolgáltatásokhoz való hozzáférésével kapcsolatos döntés.[15] Az ilyen profilalkotással, valamint automatizált adatkezelésen alapuló döntéshozatallal járó

[12] NAIH/2015/2201/17/H ügyszámú határozat, 15. o.
[13] GDPR 4. cikk 4. pontja.
[14] GDPR 22. cikk (1) bek.
[15] Az Adatvédelmi Munkacsoport Iránymutatása az automatizált döntéshozatallal és a profilalkotással kapcsolatban

Az Innovációs és Technológiai Minisztérium ÚNKP-21-3 kódszámú Új Nemzeti Kiválóság Programjának a Nemzeti Kutatási, Fejlesztési és Innovációs Alapból finanszírozott szakmai támogatásával készült.

adatkezelések esetén tehát az adatkezelő köteles az érintettet tájékoztatni az automatizált döntéshozatal tényéről, ideértve a profilalkotást is, valamint legalább ezekben az esetekben az alkalmazott logikára és arra vonatkozó érthető információkról.[16]

Természetesen a fenti automatizált döntéshozatalról, illetve profilalkotásról való tájékoztatás kötelezettségének történő megfelelés több szempontból is nehézséget okozhat. E körbe értendő az úgynevezett „feketedoboz probléma" is, amelyről alább írunk részletesebben. A fentieken túl azonban érthető módon az MI alapú megoldás működésének közérthető leírása is számos esetben problémát jelenthet, kiváltképp, ha az adott adatkezelési művelet, illetve alkalmazott technológiai különösen összetett (például: egészségi állapotra vonatkozó információk gyűjtése és komplex elemzése), illetve, ha az adott érintetti csoport szenzitívnek tekinthető vagy sajátos információ-átadást igényel (például: gyermekek, egyes fogyatékossággal élő személyek).

A fentiek kapcsán hangsúlyozandó továbbá, hogy a tájékoztatás az adatkezelés valamennyi típusa, illetve fajtája esetén kiemelt fontossággal bír, különös hangsúlyt élvez azonban az érintett hozzájárulásán alapuló adatkezelések esetén. A hozzájárulásnak ugyanis tájékoztatáson kell alapulnia[17], ennek hiányában ugyanis az érintett nem képes megfelelő döntést hozni a hozzájárulás megadásáról. A fentiek kapcsán a hozzájáruláshoz közvetlenül kapcsolódó tájékoztatásnak minimálisan ki kell térnie az adatkezelő kilétére, a vonatkozó adatkezelési művelet céljára, a gyűjtött, illetve felhasznált személyes adatokra vagy azok típusára, a hozzájárulás visszavonásának lehetőségére, az automatizált döntéshozatal céljából történő felhasználásra vonatkozó tájékoztatásra, valamint harmadik országba történő adattovábbítás esetén az adattovábbítással kapcsolatos megfelelőségi határozat, vonatkozó megfelelő garancia hiányából fakadó lehetséges kockázatokra.[18] Természetesen a fentebb írtak nem jelentik azt, hogy ezen információk megadásával az adatkezelő feltétlenül mentesülne bármely egyéb tájékoztatási kötelezettségétől. A fenti információkat ugyanis a hozzájáruló nyilatkozat részeként vagy

a 2016/679 rendelet alkalmazásához, 17/HU.WP251rev.01, 21-22. o.
[16] GDPR 13. cikk (2) bek. f) pontja, valamint 14. cikk (2) bek. g) pontja.
[17] GDPR (32) preambulum-bekezdés.
[18] Az Európai Adatvédelmi Testület 5/2020. sz. iránymutatása az (EU) 2016/679 rendelet szerinti hozzájárulásról, 17-18. o.

Az Innovációs és Technológiai Minisztérium ÚNKP-21-3 kódszámú Új Nemzeti Kiválóság Programjának a Nemzeti Kutatási, Fejlesztési és Innovációs Alapból finanszírozott szakmai támogatásával készült.

közvetlenül ahhoz kapcsoltan kell az érintett tudomására hozni, míg a további, GDPR 13, illetve 14. cikkeiben megkövetelt információkat az adatvédelmi tájékoztató részeként is az érintett tudomására lehet hozni.

Az adatkezelésről való tájékoztatás fentebb írt általánosnak mondható kötelezettsége alól azonban lehetnek kivételek is. Így például sürgős orvosi beavatkozáson áteső beteg részére értelemszerűen nem szükséges előzetes tájékoztatást nyújtani a személyes adatainak kezeléséről. Ugyancsak eltérően érvényesül a tájékoztatás gyermekek személyes adatainak kezelése esetén. Így a „*gyermekek személyes adatai különös védelmet érdemelnek, mivel ők kevésbé lehetnek tisztában a személyes adatok kezelésével összefüggő kockázatokkal, következményeivel és az ahhoz kapcsolódó garanciákkal és jogosultságokkal*”[19]. Erre tekintettel tehát a gyermekeket is életkoruknak megfelelően tájékoztatni kell személyes adataik kezeléséről az általuk értett nyelven, míg a gyermek törvényes képviselője részére az „átlagos” módon fogalmazott adatvédelmi tájékoztatót kell rendelkezésre bocsátani. Hangsúlyozandó, hogy az ilyen „gyermeknyelven” megfogalmazott tájékoztatót is életkoruknál vagy állapotuknál fogva megérteni képtelen gyermekek részére az adatkezelésről szóló tájékoztatást értelemszerűen nem szükséges megadni, esetükben elegendő a törvényes képviselő tájékoztatása.

[19] GDPR (38) preambulum-bekezdés.

Az Innovációs és Technológiai Minisztérium ÚNKP-21-3 kódszámú Új Nemzeti Kiválóság Programjának a Nemzeti Kutatási, Fejlesztési és Innovációs Alapból finanszírozott szakmai támogatásával készült.

IV. Adatkezelés technológiai környezetben

1. Átlátható adatkezelés az információs társadalomban

A modern információs társadalmakban az adatok gyűjtésére, feldolgozására és elemzésére épülő technológiák nélkül a hétköznapok nehezen elképzelhetők. A közösségi média és keresőoldalak elemzik a böngészési szokásainkat, és ezek alapján jelenítenek meg számunkra promóciós ajánlatokat vagy egyéb tartalmakat, az okostelefonunkon keresztül számos applikációval oszthatjuk meg helymeghatározási adatainkat, számos szolgáltatásért pedig az adatainkkal fizetünk vagy azért cserébe kapunk kedvezményeket vagy személyre szabott szolgáltatást. Mindez kétségtelenül kényelmesebbé teszi az életünket, azonban egyúttal kiszolgáltatottá is tesz minket, hiszen szokásaink, kapcsolataink, és végső soron a személyiségünk is feltérképezhetővé, kiaknázhatóvá válik, az adatainkból nyert információk révén pedig sok esetben befolyásolhatók lehetünk. Ennek kapcsán kiemelendő, hogy az adataink felett rendelkező legnagyobb szolgáltatók az évek során egyfajta adatmonopóliumot alakítottak ki, amelynek segítségével jelentős gazdasági és társadalmi befolyásra tettek szert. Ez kétségkívül sok esetben a piac és a társadalom széles körének járó előnyöket biztosít, hiszen például a keresőoldalak valamennyi felhasználó számára képesek hatékony és gyors találatok biztosítani, valamint a nehezen fellelhető információkat is elérhetővé tenni, továbbá a kisvállalkozások is éppúgy a nagy technológiai cégek szolgáltatásaira támaszkodhatnak, mint a multinacionális vállalatok. Azonban a nagy technológiai cégek információs erőfölény az érintettek oldalán sok esetben hátrányként jelentkezik, amelynek káros hatásai szintén nem tekinthetők elhanyagolhatónak. Ezen káros hatásokat enyhítik a személyes adatok kezelésével kapcsolatos átláthatósági követelmények, illetve tájékoztatási kötelezettségek, amelyek arra kötelezik a személyes adatokat kezelő szervezeteket, hogy információt szolgáltassanak ezen adatok kezeléséről. Ennek hála az érintettek is megfelelő tudás birtokában léphetnek fel a személyes adataik esetleges jogsértő kezelésével szemben, valamint gyakorolhatják adatvédelmi jogaikat, ideértve például a szükségtelenül kezelt adatok törlése iránti fellépést vagy a személyes adataikról történő másolat kérését.

Az Innovációs és Technológiai Minisztérium ÚNKP-21-3 kódszámú Új Nemzeti Kiválóság Programjának a Nemzeti Kutatási, Fejlesztési és Innovációs Alapból finanszírozott szakmai támogatásával készült.

A fentieken túl az átláthatóság számos egyéb előnnyel is járhat az érintett és a társadalom számára, ideértve az adatkezelő elszámoltathatóságát, az általa alkalmazott technológia és megoldások könnyebb megismerhetőségét, valamint a tisztességes piaci versenyben való előbbre jutást az átlátható adatkezelést folytató szereplők részére.

Az átláthatóság továbbá különösen jelentős súllyal érvényesül személyes adatokkal való kiemelt vagy tömeges visszaélés vagy adatvédelmi incidensek (például: hackertámadás, adathordozók elvesztése) esetén. 2019-ben például a Szövetségi Kereskedelmi Bizottság (Federal Trade Commission) eljárást indított az Equifax Inc. elnevezésű amerikai pénzügyi szolgáltató ellen. A társaság nem megfelelő intézkedéseket alkalmazott fogyasztók adatainak tárolására szolgáló rendszerének védelme érdekében, amely egy adatszivárgáshoz vezetett, elérhetővé téve körülbelül 147 millió fogyasztó személyes adatait (például: nevét, lakcímét, társadalombiztosítási számát). Mindez érthető módon az érintetteket kiemelt kockázatoknak tette ki (ideértve például: személyiséglopást vagy a személyes adataikkal való egyéb visszaélést). Az eljárás eredményeként az Equifax beleegyezett, hogy legalább 575 millió dollárt fizet a fogyasztók kárának megtérítésére, illetve további 125 millió dollárt, amennyiben az előbbi összeg a fenti cél eléréséhez nem lenne elegendő.[20] A társaságot e körben, bár számos intézkedést hozott az adatszivárgás megfékezése, valamint a károsultak segítése érdekében, az incidens körülményein kívül az esettel kapcsolatos nem megfelelő transzparencia okán is kritikák érték, ideértve például az incidens társaságon belüli nem megfelelő kommunikációját, az incidens felfedésének nagyobb botrány elkerülése érdekében való hátráltatását.[21] Ugyancsak heves kritikák érték például az Uber autómegosztó applikációt, amelytől 2016-ban egy csoport hacker szerezte meg közel 57 millió amerikai felhasználójának és sofőrjének adatait (ideértve az érintettek nevét, e-mail címét, telefonszámát, valamint a sofőrök jogosítvány adatait). Az Uber 100.000 dollárt fizetett a hackerek részére az adatok törlése, valamint az incidens eltusolása érdekében. Az Uber csak egy évvel később, egy belső vizsgálatot követően hozta nyilvánosságra a fenti incidenst. Az eset szintén hatósági fellépést eredményezett,

[20] Federal Trade Commission, Equifax to Pay $575 Million as Part of Settlement with FTC, CFPB, and States Related to 2017 Data Breach, https://www.ftc.gov/news-events/news/press-releases/2019/07/equifax-pay-575-million-part-settlement-ftc-cfpb-states-related-2017-data-breach, 2019.07.22 [2022.08.28]
[21] Thomas Brewster, How Equifax Kept Its Mega Breach Secret From Its Own Staff, Forbes, 2018.03.14, https://www.forbes.com/sites/thomasbrewster/2018/03/14/how-equifax-kept-its-mega-breach-secret-from-its-own-staff/?sh=271a34153ef1 [2022.08.28.]

Az Innovációs és Technológiai Minisztérium ÚNKP-21-3 kódszámú Új Nemzeti Kiválóság Programjának a Nemzeti Kutatási, Fejlesztési és Innovációs Alapból finanszírozott szakmai támogatásával készült.

amelynek eredményeként az Uber 148 millió dollár összegű bírság megfizetését vállalta, valamint ugyancsak vállalta, hogy megfelelő belső adatvédelmi incidenskezelési és adatbiztonsági gyakorlatot alakít ki, továbbá belső szabályokat vezet be az etikátlan munkavállalói magatartások jelentésére és külső adatbiztonsági szakértők szükség esetén való bevonására.[22]

2. Feltétlenül jó-e az átláthatóság?

Az átlátható adatkezelés a fentebb is írtak szerint számos előnnyel jár, mind az érintettek és az adatkezelő, mind általánosságban a társadalom és a gazdaság, valamint a technológiai fejlődés számára. Emellett azonban az átláthatóság hátrányokkal is járhat, ideértve többek között

- az érintettekre ható túlzott információs terhet;
- az érintett számára csak látszólag hasznos információk átadását;
- a fejlődő technológiák területén való kiszámíthatatlanság nehéz megragadását;
- gazdasági vagy biztonsági érdekeket sértő információk indokolatlan felfedését.

A fentiek kapcsán a túlzott információs teher különös problémát jelenthet az MI általi, valamint általában a technológiai környezetben járó adatkezelések területén, ahol az alkalmazott technológia és a kapcsolódó környezet, valamint folyamatok sajátosságai okán az adatkezelés nehezen foglalható össze, illetve sokszor csak bővebb kifejtés útján adható kép az adatkezelési műveletek végzéséről. Mindez az érintett számára adott esetben zavaró hatással járhat, illetve félrevezető képet tárhat elé az adatkezelésről, amely az érintettet az adatkezeléssel kapcsolatban könnyelmű vagy nem eléggé átgondolt döntés meghozatalára késztetheti.

[22] New York State Office, Attorney General, 2018.09.26, A.G. Underwood Announces Record $148 Million Settlement With Uber Over 2016 Data Breach, https://ag.ny.gov/press-release/2018/ag-underwood-announces-record-148-million-settlement-uber-over-2016-data-breach [2022.08.28]

Az Innovációs és Technológiai Minisztérium ÚNKP-21-3 kódszámú Új Nemzeti Kiválóság Programjának a Nemzeti Kutatási, Fejlesztési és Innovációs Alapból finanszírozott szakmai támogatásával készült.

A fentiekkel összhangban ugyancsak károsnak bizonyulhat a tájékoztatás, amennyiben az az érintettet ok nélküli bizakodással tölti el vagy olyan további döntés meghozatalára sarkallja, amelyet a technológia folyamatainak átláthatósága hiszemében hoz meg. A fentiekre tekintettel hangsúlyozott figyelmet kell fordítania az adatkezelőnek az érintettek megfelelő tájékoztatására fejlesztés alatt álló technológiai megoldásokhoz kapcsolódó adatkezeléseknél, és tájékoztatnia kell az érintetteket a technológia kiforratlanságából eredő kapcsolódó kockázatokról is.

Mindemellett egyes információk nyilvánosságra hozatala, az érintettel való megosztása az adatkezelő számára is jelentős hátrányokat eredményezhet, amennyiben az üzleti titoknak minősülő információk felfedéséhez vezethet, illetve az adatkezelőt biztonsági kockázatoknak teheti ki (például: az alkalmazott technológia vagy rendszer manipulálása, egyes, adatkezelő által tárolt információk könnyebb megszerzése arra jogosulatlan személyek által). E körben természetesen leszögezendő, hogy az érintettek személyes adatainak és magánszférájának védelme jellemzően felülírja az adatkezelők biztonsági vagy gazdasági érdekeit. Mindazonáltal az olyan esetekben, ahol az érintettek részére az adatkezelő technológiai környezetben folytatott adatkezelésekről ad tájékoztatást, javasolt lehet törekedni az üzleti titoknak minősülő, valamint egyéb szellemi tulajdon-védelem alá eső, illetve az adatbiztonság kapcsán kiemelt jelentőséggel bíró, az érintett személyes adatainak kezelése tekintetében kevéssé releváns információk megosztásának lehetséges körű elkerülésére.

A fentiekre tekintettel tehát megállapítható, miszerint a transzparencia az adatvédelem egyik alappillérének tekinthető, annak alkalmazása azonban nem lehet korlátlan, ugyanis ezzel vagy az adatkezelőnek okozna aránytalan sérelmet az irányadó adatvédelmi szabályozás, vagy épp az érintetteknek, akiknek a jogait és érdekeit védeni hivatott. Erre tekintettel az adatkezelésről való tájékoztatás tartalma, formája és nyelvezete a vonatkozó jogszabályi rendelkezésekre, az alkalmazott technológia sajátosságaira, valamint az adatkezelés körülményeire tekintettel határozható csak meg megfelelően, ahogy a tájékoztatás követelménye alóli esetleges kivételek köre is.

Az Innovációs és Technológiai Minisztérium ÚNKP-21-3 kódszámú Új Nemzeti Kiválóság Programjának a Nemzeti Kutatási, Fejlesztési és Innovációs Alapból finanszírozott szakmai támogatásával készült.

3. A szabályozás szerepe az átláthatóság megteremtésében

A személyes adatok kezelésével kapcsolatos átláthatóság megteremtésében jelentős szerepet játszik a megfelelő szabályozási környezet kialakítása. Ez különösen azért is fontos, mivel az adatvédelem multidimenzionális problémaként fogható fel, amelynek tükrében a személyes adat az érintett személy autonómiájához, személyiségéhez kapcsolódik vagy kapcsolható, annak érvényre juttatása pedig számos szempont figyelembevételét követeli meg.[23]

A fentiek tükrében azonban a szabályozás alatt nem csak a jogszabályalkotást érthetjük, hanem e körbe tartozónak tekinthetők egy adott iparágra vagy szakmára vonatkozó szakmai, iparági, illetve etikai szabályok, valamint egy adott szervezet által kialakított belső szabályozás is, amely például egy adott cégcsoporthoz tartozó társaságok és azok munkavállalóinak eljárásaira, viselkedésére, meghatározott ügyekkel való kapcsolatára vonatkozóan határoz meg követelményeket. A fentiek szerinti, tágan értelemezett szabályozás tehát szükséges a személyes adatok megfelelő körű védelmének kialakításához, és a társadalmi értékek védelmén túl elévülhetetlen szerepet játszik egy adott szervezet, szakma vagy iparág szereplői adatkezeléseinek az érintett természetes személyek számára történő áttekinthetővé tételében, ekképp pedig a jogszerű és etikus működés biztosításában, tekintettel arra, hogy a helyes szabályozás eredményeként elérhető, hogy az adott szervezet, annak tagjai, résztvevői, illetve az adott szakma, iparág képviselőinek személyes adatok kezelésével kapcsolatos tevékenységei kellőképpen átláthatóak legyenek, mindazonáltal a segítségével a túlzott transzparenciával járó kockázatok is elkerülhetők.

Ennek kapcsán kiemelendő, hogy a tájékoztatással kapcsolatos szabályozás hatásai csak az adott iparág, szakma, illetve szakterület megfelelő ismeretében, valamint a technológiai fejlődés hatásainak helyes felmérésével vetíthetők előre. Amennyiben ugyanis a szabályozás bizonyos információk elérhetővé

[23] Monroe E. Price, Stefaan G. Verhulst, Libby Morgan (szerk.): Routledge Handbook of Media Law, Routledge, Oxford, New York, 2013, 467. o.

Az Innovációs és Technológiai Minisztérium ÚNKP-21-3 kódszámú Új Nemzeti Kiválóság Programjának a Nemzeti Kutatási, Fejlesztési és Innovációs Alapból finanszírozott szakmai támogatásával készült.

tételét előírja, azonban ezeket a szabályozott szervezetek vagy személyek „papírforma” szerint, az érintetteknek a vonatkozó lényeges kockázatokról való tájékoztatása nélkül teljesíthetik, úgy a tájékoztatás követelménye súlytalan marad. Negatív példaként tekinthetők e körben az Egyesült Államokban népszerűnek számító, azonban a világ számos más pontján is sokak által használt online befektetési applikációk, amelyek számos esetben jelentős tartozásokat eredményeznek az azokat használó, pénzügyi ismeretekkel nem rendelkező személyek számára. Mindez jellemzően abban az esetben is igaz, ha a vonatkozó applikációk üzemeltetői megfelelnek a vonatkozó szolgáltatókra irányadó jogszabályi, illetve hatósági előírásoknak, tekintettel arra, hogy a laikus felhasználók hajlamosak elbizakodottan dönteni hasonló helyzetben, a fenti applikációk által generált reklámok pedig – a kockázatokról, valamint a személyes adatok felhasználásáról való megfelelő tájékoztatás hiányában – a számos esetben elnagyolt felhasználói várakozásokat csak tovább erősítik. 2020-ban például egy fentiek szerinti applikációt használó 20 éves fiatalember öngyilkossága rázta meg az amerikai közvéleményt. A fiatalember egy Robinhood nevű befektetési alkalmazást használt, amelyen keresztül többszázezer dollárnyi veszteséget halmozott fel. Ennek kapcsán az alkalmazást számos kritika érte, mivel lehetővé tették képzetlen, a pénzügyi piacok működését nem ismerő felhasználók számára hatalmas összegű adósság felhalmozását, anélkül, hogy ennek kapcsán előzetesen kellő tájékoztatást nyújtottak volna a kellő kockázatokról[24]. Ezen alkalmazások emellett a fentieken túl számos adatot gyűjtenek a felhasználók befektetési, kockázatvállalási szokásairól is, amelyeket sok esetben a még nagyobb felhasználószám elérése, valamint személyre szabott reklámok küldése, kockázatvállalás serkentése érdekében használnak fel, tovább növelve az érintettekre ható esetleges negatív hatásokat. Mindezen kockázatok köre összetett szabályozási hozzáállással lenne csökkenthető, ideértve például a hasonló befektetési alkalmazások nyújtóira vonatkozó fokozott tájékoztatási előírást, valamint az adatok felhasználásával kapcsolatos etikus korlátokat (például: a felhasználói viselkedési adatok felhasználásának tilalmát a felhasználók kockázatos befektetések megtételére vonatkozó „rábeszélésére”). Mindez természetesen csak egy szempontként értékelhető egy szolgáltatás-típus kapcsán, azonban a hasonló egységes megközelítési módszer elengedhetetlen a tájékoztatás tartalmának helyes kialakítása kapcsán, más szolgáltatások vagy megoldások esetén is.

[24] Yasmin Khorram, Kate Rooney, Young trader dies by suicide after thinking he racked up big losses on Robinhood, CNBC, 2020.06.18, https://www.cnbc.com/2020/06/18/young-trader-dies-by-suicide-after-thinking-he-racked-up-big-losses-on-robinhood.html [2022.08.28]

Az Innovációs és Technológiai Minisztérium ÚNKP-21-3 kódszámú Új Nemzeti Kiválóság Programjának a Nemzeti Kutatási, Fejlesztési és Innovációs Alapból finanszírozott szakmai támogatásával készült.

Megemlítendő továbbá, hogy a személyes adatok kezelésével kapcsolatos transzparencia megteremtése kapcsán különösen fontos az adatkezelés változó körülményeinek figyelembevétele, ekként például számos, adott esetben triviálisnak tűnő adat (például: áruházi bevásárlások) gyűjtésével és rendszerezésével kifejezetten szenzitív információkra is levonható következtetés (például: ételallergia, betegségek),[25] így amennyiben az adatkezelő az ilyen információkat jogszerűen is gyűjtheti és dolgozhatja fel, e tekintetben nagyobb hangsúlyt kell fektetnie az adatkezelés céljának és egyéb lényeges jellemzőinek ismertetésére. Mindez kiváltképpen igaz az olyan megoldásokra (például: magáncélú kommunikációra vagy intim helyzetekben használt megoldások), amelyek az érintettekről szexuális életük vagy egyéb kifejezetten a magánszféra körébe tartozó tevékenységeik során gyűjtenek információkat.[26]

Hangsúlyozandó továbbá, hogy az MI, illetve robotok szabályozása kapcsán különösen fontos szempontot képez az MI, illetve a robot autonómiája mint az önálló döntéshozatali képesség foka; ekként a szabályozás mélységének is az autonómia mértékéhez kell igazodnia ezen új technológiák esetén.[27] Mindez természetesen a fenti technológiák általi adatkezelésre is irányadó, ahol az általános mellett ágazati vagy speciális szabályok bevezetése növelheti a szabályozás differenciáját, valamint segíthet kialakítani a megfelelő adatkezelés gyakorlatot.

4. Az önszabályozás jelentősége

Az adott szakma, tevékenység vagy iparág szereplői általi önszabályozás számos területen kiemelt jelentőséggel bír, ideértve például a marketing- vagy a gyógyszeripart, illetve a sajtót és a médiát, amelyek tevékenységük sajátosságaira tekintettel már korábban is számos esetben kiemelt figyelmet fordítottak a személyes adatok kezelésére. Mindemellett az önszabályozás a vállalati szférában eltérő

[25] Paul Bernal, Internet privacy rights: rights to protect autonomy, Cambridge University Press, New York, 2014, 34. o.
[26] Danielle Keats Citron, The Roots of Sexual Privacy: Warren and Brandeis & the Privacy of Intimate Life, The Columbia journal of law and the arts, 42/3, 2019, 385. o.
[27] Klein Tamás, Tóth András (szerk.): Technológia jog – Robotjog – Cyberjog, Wolters Kluwer Hungary, Budapest, 2018, Klein Tamás: Második rész: Robotjog, 179-215. o., 183. o.

Az Innovációs és Technológiai Minisztérium ÚNKP-21-3 kódszámú Új Nemzeti Kiválóság Programjának a Nemzeti Kutatási, Fejlesztési és Innovációs Alapból finanszírozott szakmai támogatásával készült.

típusú vállalkozások esetén is már hosszú évekkel ezelőtt megjelent, ideértve az egyes nagyvállalatok széles körben használt etikai és magatartási kódexeit, amelyek sok esetben a személyes adatok védelmével, valamint az adatok felhasználásával kapcsolatos átláthatóságra vonatkozóan is tartalmaznak előírásokat.

Jelenleg azonban kijelenthető, hogy az önszabályozás a technológiai környezetben még kevésbé tekinthető elterjedtnek. Ennek okai közé sorolható – többek közt – az MI alapú vagy egyéb technológiák kiforratlansága, illetve rapid fejlődése, nehéz szabályozhatósága, a hiányzó jogszabályi környezet, valamint a szabályozás technológiai fejlődésre, gazdasági eredményességre gyakorolt negatív hatásaitól való félelem. Hangsúlyozandó azonban, hogy az önszabályozás a technológiai megoldások területén is több szempontból előnyös lehet az adott szektor szereplőinek, mivel növelheti a társadalom bizalmát az adott megoldások és azok alkalmazói iránt, valamint megelőzheti az adott esetben szigorúbb jogalkotást vagy hatósági fellépést, nagyobb teret engedve az adott szakmai vagy piaci szereplők álláspontjainak érvényesülésére. A nem megfelelő önszabályozási törekvések ezzel szemben különösen károsak lehetnek, és jelentősen ronthatják egy-egy megoldás társadalmi, illetve hatósági vagy szabályozói megítélését. Ennek kapcsán példaként említhetők a reklámipar ún. real-time bidding elnevezésű reklámfelület értékesítési megoldások kapcsán tett önszabályozási törekvései, amelyek a fenti tevékenységet folytatók működését igyekeztek összhangba hozni az európai adatvédelmi jogszabályi követelményekkel. Ennek körében az Interactive Adverting Bureau Europe (IAB) nevű reklámipari szervezet létrehozott egy Transparency & Consent Framework elnevezésű mechanizmust, amelyen keresztül a weboldalak látogatói online járulhatnak hozzá személyes adataik kezeléséhez vagy tiltakozhatnak az ellen. A mechanizmus azonban nehézkes átláthatóságot és lényegében nem megfelelő tájékoztatáson alapuló hozzájárulások beszerzését eredményezte az egyébként is erősen technikai, az átlagos felhasználó által nehezen megérthető real-time bidding rendszerek esetén. A mechanizmust ekként a belga adatvédelmi hatóság jogsértőnek találta, és többek között – az átlátható adatkezelés biztosításának hiánya miatt – 250.000 euró összegű adatvédelmi bírságot szabott ki a szervezetre.[28] Ennek kapcsán természetesen felvetődhet azon kritika, miszerint a kreatív, gazdaságilag adott esetben hasznos megoldásoknak nagyobb teret

[28] A belga adatvédelmi hatóság (Autorité de protection des données) DOS-2019-01377 sz. ügyben hozott döntése, https://www.autoriteprotectiondonnees.be/publications/decision-quant-au-fond-n-21-2022-english.pdf [2022.08.28]

Az Innovációs és Technológiai Minisztérium ÚNKP-21-3 kódszámú Új Nemzeti Kiválóság Programjának a Nemzeti Kutatási, Fejlesztési és Innovációs Alapból finanszírozott szakmai támogatásával készült.

szükséges hagyni, és az adatvédelemnek nem lehet célja, hogy a reklámipari innováción indokolatlanul megkösse.[29] Mindemellett azonban azt is fontos kiemelni, miszerint a reklámipari szereplők jogszerű és etikus adatkezelési gyakorlat kialakítására bírása végsősoron gazdasági előnyökkel is jár, hiszen növeli a szereplőkbe vetett bizalmat, tevékenységüket pedig áttekinthetővé teszi. Erre tekintettel adott esetben indokolt lehet hasonló, akár kifejezetten szigorúnak mondható szankció alkalmazása is, azonban természetesen idővel ki kell alakulni olyan hatékony adatvédelmi hatósági gyakorlatnak és iránymutatásnak, amely egyben a reklámipari önszabályozással együtt vezethet el egy sikeres, adatvédelmi követelményeknek is megfelelő reklámipari gyakorlathoz.

[29] Dr. Pázmándi Kinga, Modern reklámjog. A reklám a tisztességtelen verseny elleni jog és a modern reklámjog határán, HVG-ORAC Lap- és Könyvkiadó, Budapest, 2007, 18. o.

Az Innovációs és Technológiai Minisztérium ÚNKP-21-3 kódszámú Új Nemzeti Kiválóság Programjának a Nemzeti Kutatási, Fejlesztési és Innovációs Alapból finanszírozott szakmai támogatásával készült.

V. Az egyes technológiák átláthatóságával kapcsolatos szempontok

1. A mesterséges intelligencia általi adatkezelés

a) A mesterséges intelligencia meghatározása, szabályozásának jelentősége

A mesterséges intelligencia (MI) *„mint a betáplált adatok alapján önmagukat tanítani és javítani képes algoritmikus rendszerek összessége”*[30], az emberi alkotóképesség és leleményesség egyik legfelsőbb fokát testesíti meg, amelyet elsőként az irodalom és a művészetek nagyjai álmodtak meg, a tudományt megelőzve, amely a fenti előzmények nyomán fokozatosan fedezte fel magának azt.[31] Az MI kétségtelenül számos lehetőséges rejt magában. Így alkalmas lehet arra is, hogy az emberiség általános segítőjévé váljon, és számos technikai, illetve épp ismétlődő, monoton munkavégzést vagy nagyfokú, komplex elemzések elvégzését igénylő területen is képes támogatni az embert, ideértve számos a kutatási-fejlesztési feladatok támogatását, a rendszeres elemzések, vagy épp a korábbi számítógépek képességeit meghaladó számítási feladatok elvégzését.

A mesterséges intelligencia azonban megfelelő szabályozás nélkül, különösen annak egy magasabb fejlettségi szintjét szemlélve, a társadalom számára kiemelt kockázatokat is magában rejthet. Nem nehéz ugyanis belátni, hogy egy önvezető autó által okozott halálos baleset, egy pénzügyi algoritmus számítási hibája folytán végzett veszteséges befektetés vagy egy tartalomgyártáshoz használt MI megoldás általi szerzői jogsértés mind-mind komplex felelősségi kérdésekhez vezetnek, amelyek megválaszolásához nem feltétlenül nyújtanak kellő támpontot az általános jogi elvek, vagy a büntető-, illetve a polgári felelősség jelenlegi szabályai.

A fentiekre tekintettel a mesterséges intelligencia szabályozása a világ számos pontján kulcskérdéssé vált az elmúlt időszakban. Mind a mesterséges intelligenciával kapcsolatos nemzeti stratégiák, etikai

[30] Magyarország Mesterséges Intelligencia Stratégiája, https://ai-hungary.com/api/v1/companies/15/files/137203/view, 6. o.
[31] Necz Dániel, A mesterséges intelligencia hatása a szerzői jogra, Iparjogvédelmi és Szerzői Jogi Szemle, 2018/6, 52-53. o.

Az Innovációs és Technológiai Minisztérium ÚNKP-21-3 kódszámú Új Nemzeti Kiválóság Programjának a Nemzeti Kutatási, Fejlesztési és Innovációs Alapból finanszírozott szakmai támogatásával készült.

állásfoglalások, mind konkrét jogszabály-tervezetek nagy számban jelentek meg, célul tűzve ki a mesterséges intelligencia szabályozási kereteinek, etikus alkalmazásának meghatározását. A szabályozással kapcsolatos lendületet jól példázza a Gazdasági Együttműködési és Fejlesztési Szervezet (OECD) összesítése, amely szerint a világ közel 60 országában több mint 700 mesterséges intelligencia szabályozási megoldás jelent már meg[32].

Az Amerikai Egyesült Államokban a 2021. január 1-én hatályba lépő National Artificial Intelligence Initiative Act[33] vezette be az Egyesült Államok MI stratégiájának is tekinthető National Artificial Intelligence Initiative-et, amely meghatározza az MI szabályozás célkitűzéseit, egyúttal különböző stratégiai pilléreket is lefektet a pontosabb tervezés és a szabályozási és stratégiai tevékenységek összehangolása érdekében, ideértve különösen az MI-vel kapcsolatos kutatást és fejlesztést, az oktatást és a tudásmegosztást. Emellett a stratégia egyes szakterületeken is meghatározza az MI szerepét, valamint a kapcsolódó célokat, ideértve a mezőgazdaságot, a pénzügyi szolgáltatásokat, az egészségügyet, valamint a nemzetbiztonságot és a tudományt is.[34]

A fentieken túl szintén kiemelendő az Algorithmic Accountability Act[35] elnevezésű törvény tervezete, amely hatásvizsgálat elkészítését és dokumentálását, valamint egyéb intézkedések megtételét (például: adatbiztonság intézkedések garantálása) írja elő az MI alapú döntéshozatalt alkalmazó szervezeteknek (például: MI alapú hitelbírálatot alkalmazó pénzügyi szolgáltatók részére), annak érdekében, hogy a fenti MI alapú döntéshozatallal járó diszkriminációs hatásokat enyhítse, és a technológia alkalmazását átláthatóvá tegye az az általa érintett személyek részére.

Az amerikai szabályozás mellett természetesen az európai szabályozás is kiemelt lépéseket tett a mesterséges intelligencia szabályozása érdekében. Így a 2021-ben megjelent az ún. Mesterséges

[32] OECD.AI. National AI policies & strategies, https://oecd.ai/en/dashboards, 2022.08.16.
[33] National Artificial Intelligence Initiative Act, https://www.congress.gov/116/crpt/hrpt617/CRPT-116hrpt617.pdf#page=1210 [2022.08.30]
[34] National Artificial Intelligence Initiative, https://www.ai.gov/ [2022.08.30]
[35] Algorithmic Accountability Act, https://www.congress.gov/bill/117th-congress/house-bill/6580/text [2022.08.30]

Az Innovációs és Technológiai Minisztérium ÚNKP-21-3 kódszámú Új Nemzeti Kiválóság Programjának a Nemzeti Kutatási, Fejlesztési és Innovációs Alapból finanszírozott szakmai támogatásával készült.

Intelligenciáról szóló Jogszabály tervezete[36] átfogó módon kategorizálja a különböző MI alapú megoldásokat, és annak az érintettekre, valamint a társadalomra gyakorolt hatásai szerint különböző követelményeket vagy épp tilalmakat állít fel. Így első körben a tervezet tilosnak nyilvánítja az olyan MI-rendszerek révén alkalmazott technikákat, amelyek tudat alatt vagy az érintettek szenzitív jellemzőit kihasználva torzítják azok magatartását, továbbá szintén tiltja a közösségi pontozás céljára használt MI alkalmazást, valamint a biometrikus azonosító rendszerek bűnüldözési célú használatát. Ekként a tervezet az olyan felhasználási módoknak igyekszik gátat szabni, amelyek különös veszélyt jelentenek a demokratikus társadalmak működésére, valamint az érintettek magánszférájára. A fentiek mellett a tervezet a további MI alapú megoldásokat négy kockázati osztályba sorolja, különböző követelményeket és elvárásokat támasztva a különböző megoldások felé, a vonatkozó kockázatok súlyát is figyelembe véve. Ezen belül is kiemelt figyelmet szentel a tervezet az ún. nagy kockázatú MI-rendszereknek (például: biometrikus azonosításra szolgáló rendszerek vagy a jellemzően bűnüldözési célból használt MI-rendszerek), amelyekhez a leginkább jelentős követelmények társulnak.

Kiemelendő, hogy a tervezet a nagy kockázatú, illetve bizonyos egyéb MI-rendszerek kapcsán tájékoztatási követelményeket is megállapít, annak érdekében, hogy az érintettek a fenti rendszerek alkalmazásáról, valamint azok érintettekre gyakorolt hatásairól kellő információval rendelkezhessenek; e körben a tervezet – többek között – megköveteli a nagy kockázatú MI-rendszerekhez megfelelő használati utasítás mellékelését, valamint ezen MI-rendszerek várható élettartamáról, a megfelelő működés biztosításához szükséges karbantartási és gondozási intézkedésekről szóló tájékoztatást is.[37]

Emellett a tervezet szintén átláthatóságot követel meg természetes személyekkel való interakcióra szánt MI-rendszerek, továbbá az érzelemfelismerő rendszerek vagy a biometrikus kategorizálási rendszerek tekintetében, amelyek kapcsán a velük kapcsolatban álló, illetve kapcsolatba kerülő személyeket szükséges tájékoztatni. A tervezet továbbá előírja a megtévesztőnek ható deepfake tartalmak készítői

[36] Javaslat, az Európai Parlament és a Tanács Rendelete a mesterséges intelligenciára vonatkozó harmonizált szabályok (a mesterséges intelligenciáról szóló jogszabály) megállapításáról és egyes uniós jogalkotási aktusok módosításáról, Brüsszel, 2021.4.21. COM(2021) 206 final, 2021/0106(COD)
[37] A mesterséges intelligenciáról szóló jogszabály tervezet 13. cikke.

Az Innovációs és Technológiai Minisztérium ÚNKP-21-3 kódszámú Új Nemzeti Kiválóság Programjának a Nemzeti Kutatási, Fejlesztési és Innovációs Alapból finanszírozott szakmai támogatásával készült.

számára is az adott tartalom mesterséges voltáról vagy manipulálásáról való tájékoztatást. Hangsúlyozandó azonban, hogy a fenti tájékoztatási kötelezettség alól a tervezet több kivételt is megállapít, ideértve a törvényen alapuló, bűnüldözési célú, valamint a véleménynyilvánítás szabadságához, továbbá a művészet és tudomány szabadságához való jog gyakorlásához szükséges körű felhasználását.[38]

b) A mesterséges intelligencia és a transzparencia, az adatkezelés sajátosságai

A mesterséges intelligencia a technológia jellemzői okán sajátságosan viszonyul a személyes adatok védelméhez. Tekintettel arra, hogy az MI fejlesztéséhez jelentős adattömegek elemzésére van szükség, amelyek számos esetben személyes adatokat is tartalmaznak, így a megfelelő MI fejlesztéshez és alkalmazáshoz gyakran elengedhetetlennek tekinthető a kiterjedt mértékű, gyakran komplex elemzési műveleteket is magában foglaló adatkezelés.

A fentiekre tekintettel különös kihívást jelent a megfelelő tájékoztatási gyakorlat kialakítása tekintetében a fekete doboz (black box) probléma, amely sok esetben a mesterséges intelligencia döntéseinek bizonytalan kimenetelét emeli ki. Így a mesterséges intelligencia alkalmazása esetén sokszor még az algoritmust létrehozó szakemberek sem tudják előre látni, hogy az milyen eredményre is jut, illetve, hogy az MI hogyan jutott a meglévő adatok alapján egy adott következtetésre.[39] A norvég adatvédelmi hatóság jelentése e körben kiemeli, miszerint a norvég adóhatóság bevezetett egy MI alapú megoldást azon adóbevallások kiszűrésére, amelyek alaposabb vizsgálatot igényelnek. A hatóság azonban nyilvánosan elismerte, hogy egyes esetekben nem tudja pontosan megindokolni, hogy a megoldás miért emel ki egy-egy adóbevallást, tehát azt sem, hogy adott esetben miért jut téves következtetésre. Ennek kapcsán a norvég adatvédelmi hatóság kiemelt kritikaként emelte ki azon tényt, hogy az adóhatóság alul

[38] A mesterséges intelligenciáról szóló jogszabály tervezet 52. cikke.
[39] A Norvég Adatvédelmi Hatóság Mesterséges Intelligencia és Adatvédelem című Jelentése (https://www.datatilsynet.no/globalassets/global/english/ai-and-privacy.pdf) [2022.08.26], 12. o.

Az Innovációs és Technológiai Minisztérium ÚNKP-21-3 kódszámú Új Nemzeti Kiválóság Programjának a Nemzeti Kutatási, Fejlesztési és Innovációs Alapból finanszírozott szakmai támogatásával készült.

becsülte a feketedoboz probléma jelentőségét, így könnyelműen fogadja el a megoldás téves következtetéseit az érintettek, adott esetben vétlen adófizetők kárára.[40]

c) A deepfake és az átláthatóság

A deepfake a mesterséges intelligencia egy sajátos alkalmazása, amely egy személy képmásának vagy hangjának felhasználásával hoz létre neki tulajdonítható kép-, illetve hang- vagy videófelvételeket. A deepfake technológia elsőként 2017-ben jelent meg, és kezdetben főként híresség arcképének felhasználásával létrehozott pornográf felvételek készítéséhez használták[41], azonban a deepfake hamar utat talált más területekre is, ideértve többek között a szórakoztató- és a reklámipart. A deepfake emellett más területekre is gyorsan utat talált, adott esetben sokkoló vagy megdöbbentő alkalmazási módokat is ideértve. Így például a MyHeritage nevű családfakutatással foglalkozó weboldal DeepNostalgia elnevezésű alkalmazása képes elhunyt családtagok régi fényképeit „élővé" varázsolni[42]. Várhatóan a hasonló megoldások a jövőben is meghatározók lesznek, és egyre több ilyen tartalom lesz majd elérhető az arra fogékony közönségnek.

Természetesen az MI szabályozása és az MI általi adatkezelés kapcsán írtak a deepfake esetén is irányadónak tekinthetők. A deepfake esetén azonban a személyes adatok védelmének különös hangsúllyal kell érvényesülnie, tekintettel arra, hogy a deepfake sok esetben valós személyek arcképét és hangját használja fel újabb tartalmak létrehozására, a segítségével pedig szinte bármely személynek tulajdoníthatók olyan mondatok vagy tettek, amelyeket az illető a valóságban sohasem mondott vagy követett el. Így a deepfake tartalmak alkalmasak lehetnek, és adott esetben befolyásolhatók a politikai élet szereplőinek lejáratására, választások befolyásolására, a kérdéses hitelességű tartalmak elterjedése pedig a közügyek iránti érdeklődés tömeges csökkenéséhez is vezethet, végső soron nagyban korlátozva

[40] Uo., 12-13. o.
[41] Dave Johnson, What is a deepfake? Everything you need to know about the AI-powered fake media, 2022.08.10, https://www.businessinsider.com/what-is-deepfake, 2022.08.16.
[42] Jane Wakefield, MyHeritage offers 'creepy' deepfake tool to reanimate dead, 2021.02.26, https://www.bbc.com/news/technology-56210053, 2022.08.16.

Az Innovációs és Technológiai Minisztérium ÚNKP-21-3 kódszámú Új Nemzeti Kiválóság Programjának a Nemzeti Kutatási, Fejlesztési és Innovációs Alapból finanszírozott szakmai támogatásával készült.

a demokratikus közbeszéd fenntartását.[43] Mindemellett a deepfake technológia alkalmas személyiséglopással kapcsolatos csalások és hasonló visszaélések elkövetésére is. Erre tekintettel különösen fontos, hogy a deepfake alkalmazások gyártói tájékoztassák a felhasználóikat, illetve weboldalukon, közösségi média alkalmazásaikon keresztül a nyilvánosságot is arról, hogy a megoldásuk milyen hatással bírhat az érintettekre. Szintén fontos továbbá, hogy egyfajta önszabályozás vagy adatbiztonsági minimumsztenderd is kialakuljon a deepfake alkalmazások piacán, amely segíthet gátat szabni a technológiával kapcsolatos visszaéléseknek, például deepfake felismerő algoritmusok kialakításának fokozott támogatásával.

A deepfake tartalmak, valamint ahhoz kapcsolódóan a dezinformáció elleni küzdelem kapcsán a fentieken túl figyelemre méltó szabályozási kezdeményezéseket is megfigyelhetünk. Az Egyesült Államokban például Kalifornia állam két törvényt fogadott el 2019 végén, amelyek a deepfake technológia hamis pornográf felvételek létrehozására, illetve választási célú befolyásolásra történő felhasználását tiltják és szankcionálják, a technológia társadalmilag hasznos alkalmazását (például: szatíra vagy karikatúrák létrehozására történő felhasználását) azonban nem korlátozzák.[44]

A fentiek kapcsán kiemelendő, hogy az európai szabályozás is célul tűzte ki a dezinformáció, valamint ennek kapcsán a káros deepfake tartalmak elleni fellépést, amely mind a személyes adatok védelmére vonatkozó jogi szabályozásban, mind a digitális szolgáltatásokra vonatkozó változó jogszabályi környezetben megmutatkozik. Így az európai uniós adatvédelmi szabályozás, ideértve különösen a GDPR szabályait, kiemelt előnyben részesíti az azonosított vagy azonosítható természetes személyekre vonatkozó információk védelmét[45], amely kiterjed az érintettre vonatkozóan létrehozott, adott esetben hamis vagy félrevezető tartalmakra, így például beazonosítható érintettre vonatkozó deepfake felvételekre is. Emellett az EU digitális szolgáltatásokról szóló jogszabály tervezete is kiemeli, miszerint *„Figyelembe kell venni … a rendszerszintű kockázatok által a társadalomra és a demokráciára gyakorolt*

[43] Mráz Attila, Deepfake, demokrácia, kampány, szólásszabadság, 249-277. o. In: Török Bernát, Ződi Zsolt (szerk.), A mesterséges intelligencia szabályozási kihívásai, Ludovika Egyetemi Kiadó, Budapest, 2021, 257. o.
[44] California Legislative Information, https://leginfo.legislature.ca.gov/faces/billNavClient.xhtml?bill_id=201920200AB730, 2022.08.19.
[45] GDPR 4. cikk 1. pontja.

Az Innovációs és Technológiai Minisztérium ÚNKP-21-3 kódszámú Új Nemzeti Kiválóság Programjának a Nemzeti Kutatási, Fejlesztési és Innovációs Alapból finanszírozott szakmai támogatásával készült.

lehetséges negatív hatásokat, például a félretájékoztatást vagy a manipulatív és visszaélésen alapuló tevékenységeket. Idetartoznak az információk, beleértve a félretájékoztatást, fokozott terjesztésére irányuló összehangolt tevékenységek – például botok vagy hamis fiókok használata hamis vagy félrevezető információk előállítására, néha gazdasági előnyszerzés céljából –, amelyek különösen károsak a szolgáltatások veszélyeztetett igénybe vevői, például a gyermekek esetében".[46]

d) A mesterséges intelligencia által, illetve segítségével alkotott egyéb művek sajátosságai

Az MI alkalmazása a művészet és az irodalom területén átformálja mindazt, amit korábban az emberi alkotásról gondoltunk. Az MI ugyanis napjainkban már képes például filmet készíteni vagy regényt írni. Az ilyen műveket megillető védelem köre azonban kérdésesnek tekinthető. Az Egyesült Államok Szerzői Jogi Irodája 2019-ben és 2022-ben is arra a megállapításra jutott például, hogy MI által alkotott művek nem élvezhetnek szerzői jogi védelmet, tekintettel arra, hogy ez csak az emberi alkotók által létrehozott művekre vonatkozhatnak.[47] Ez összhangban van azzal a szintén 2022-ben hozott amerikai felsőbírósági döntéssel is, amely szerint csak az emberi feltalálók találmányai szabadalmaztathatók, így az MI által létrehozott találmányok ennek okán nem részesülhetnek szabadalmi oltalomban.[48] Habár ezen döntések az MI alkotóképességével és az MI által létrehozott művek oltalmazhatóságával kapcsolatos vitát értelemszerűen nem zárják le, azokból vitán felül kiolvasható azon nézőpont, amely szerint az MI által alkotott művek más megítélés alá esnek, mint az emberi alkotások. Mindez azonban egyéb jogi kérdéseket is felvet, ideértve adott esetben az adatvédelmi megfelelés kérdését is. Így amennyiben egy MI alkot egy videót meglévő felvételek elemzésével, az ezeken szereplő személyeket más adatkezelésekhez hasonlóan megilleti a személyes adatok védelme, az adatkezelő pedig főszabályként ezen érintettek tájékoztatására köteles a személyes adataik kezeléséről, valamint az adatkezelés egyéb, fentebb már kiemelt jellemzőiről. Ugyancsak szükséges lehet például egy zenemű szerzőjének vagy egy

[46] Javaslat az Európai Parlament és a Tanács rendelete a digitális szolgáltatások egységes piacáról (digitális szolgáltatásokról szóló jogszabály) és a 2000/31/EK irányelv módosításáról, Brüsszel, 2020.12.15., COM(2020) 825 final, 2020/0361(COD), (68) preambulum-bekezdése.
[47] Copyright Review Board, United States Copyright Office, decision, correspondence ID 1-3ZPC6C3; SR # 1-7100387071, 2022.02.14, https://www.copyright.gov/rulings-filings/review-board/docs/a-recent-entrance-to-paradise.pdf, 4. o.
[48] Thaler v. Vidal, No. 21-2347 (Fed. Cir. 2022).

Az Innovációs és Technológiai Minisztérium ÚNKP-21-3 kódszámú Új Nemzeti Kiválóság Programjának a Nemzeti Kutatási, Fejlesztési és Innovációs Alapból finanszírozott szakmai támogatásával készült.

regény írójának tájékoztatására, amennyiben MI alapú megoldással elemzik annak műveit abból a célból, hogy hasonló további műveket hozzanak létre, vagy egy új stílusban szerzett vagy írt művet hozzanak létre korábbi alkotók munkáira támaszkodva. Hangsúlyozandó azonban, hogy a tájékoztatás kötelezettsége ilyen esetben jellemzően csak akkor merülhet fel, ha kevés számú alkotó érintett. [*].

Az MI a tudomány területén is jelentős segítséget nyújthat, például elemző vagy forráskereső feladatok elvégzésével, így támogatva a tudomány szabadságát. Kiemelendő azonban, hogy a tudomány szabadsága önmagában is vitás területnek tekinthető, mind annak meghatározása, mind az annak érvényesítésére jogosult személyek körének pontos behatárolása kapcsán.[49] Így napjainkban még kérdésesnek tekinthető, hogyan hat majd az MI a tudományos életre, azonban a fentiek szerint említett körben komoly támogatást jelenthet az egyes, különösen jelentős forrásanyag feldolgozását igénylő kutatások területén.

e) A mesterséges intelligencia alkalmazása a munkahelyeken

Az MI alkalmazása értelemszerűen a munka világában is egyre jelentősebb hatásokkal bír, ideértve mind az ember által ellátandó munkakörök alakulását, mind a toborzás és a napi feladatvégzés területét. Mindezt alátámasztja a World Economic Forum 2020. októberében készült riportja is, amely szerint 2025-re 85 millió feladatot vesznek át a gépek az embertől, ugyanakkor azonban 97 millió új, ember által végzendő feladat jön majd létre.[50] Mindezen előrejelzések ugyanakkor meg is cáfolják azon gyakori félelmeket, miszerint a mesterséges intelligencia egyre fokozódó elterjedése tömeges munkanélküliséget idéz majd elő. Valójában inkább a munkakörök átstrukturálásáról beszélhetünk, ahol az adatelemzéssel kapcsolatos és az MI-vel való együttműködést igénylő, illetve a kreatív feladatok végzését megkövetelő munkakörök felértékelődnek, az egyszerűbb és monotonabb feladatok MI általi

[49] Eric Barendt: A tudomány szabadsága és a jog. Összehasonlító tanulmány (ford. Csertő István), Budapest, 2017 (az alábbi mű alapján: Academic Freedom and the Law – A Comparative Study. Hart Publishing, Oxford and Portland, Oregon, 2010), 15. o.
[50] World Economic Forum, The Future of Jobs Report, 2020. október, https://www.weforum.org/reports/the-future-of-jobs-report-2020/digest [2022.09.06.]

Az Innovációs és Technológiai Minisztérium ÚNKP-21-3 kódszámú Új Nemzeti Kiválóság Programjának a Nemzeti Kutatási, Fejlesztési és Innovációs Alapból finanszírozott szakmai támogatásával készült.

átvételével pedig akár már a munkaerőpiacra frissen belépő fiatalok is kihívással teli, motiváló munkaköröket tölthetnek be.[51]

Mindez azonban nem jelenti azt, hogy az MI által vagy annak révén vezérelt átmeneti időszak konfliktusoktól mentesen fog zajlani vagy valamennyi munkavállaló számára pozitív végkimenetellel bír majd, különösen ideértve a könnyen kiváltható, egyszerűbb feladatok elvégzését igénylő munkaköröket. Így az ilyen munkakörök betöltőit elsősorban új munkakör betöltése, a szükséges átképzés révén kell majd támogatnia a munkáltatóknak, valamint a társadalomnak az átmeneti időszak során.

A fentiek alapján kétségtelen, hogy az MI elterjedése a munkahelyeken jelentős munkaszervezési és munkajogi, valamint társadalombiztosítás kérdéseket vet fel, azonban adatvédelmi szempontból is figyelmet igényel. Így az olyan munkakörök esetén azonban, ahol az MI-vel való együttműködés vagy az MI alkalmazása révén a technológiát személyes adatok kezelésére használják, az átlátható adatkezelés követelménye – kiváltképp a munkavállalók szenzitívebb, kiszolgáltatottabb helyzete, valamint az MI általi adatkezelés kiterjedt, az érintettek személyes adatainak védelméhez való jogára kiemelt behatással bíró természetére – fokozottabb súllyal kell, hogy érvényesüljön.

A fentiekre tekintettel az MI általi toborzás esetén az álláspályázatok feletti döntéssel kapcsolatos kizárólagos gépi döntés kerülendő, azonban az érintett pályázókat ez esetben is egyértelműen tájékoztatni szükséges még jelentkezésük előtt arról, hogy a toborzáshoz MI alapú megoldást használnak. A tájékoztatásnak ki kell terjedni az említett megoldás alkalmazásának az érintettek jelentkezésére, az álláspályázat sikeres betöltésére gyakorolt hatásaira, valamint arra is, hogy emberi döntéshozó bevonására, emberi felülvizsgálatra mikor, illetve milyen körülmények esetén kerül sor.

[51] Nahia Orduña, Why Robots Won't Steal Your Job, 2021.03.19, https://hbr.org/2021/03/why-robots-wont-steal-your-job [2022.09.06]

Az Innovációs és Technológiai Minisztérium ÚNKP-21-3 kódszámú Új Nemzeti Kiválóság Programjának a Nemzeti Kutatási, Fejlesztési és Innovációs Alapból finanszírozott szakmai támogatásával készült.

Az MI megfelelő toborzási célú alkalmazásán túl természetesen az is fontos, hogy az MI alkalmazására a munkaviszony fennállása alatt, valamint megszűnésekor is a vonatkozó adatvédelmi követelményeknek megfelelően kerüljön sor. Hangsúlyozandó, hogy a munkavállalók ellenőrzése MI alkalmazásával az esetek jelentős részében profilalkotáshoz[52] vezethet a GDPR tükrében, tekintettel arra, hogy az ilyen megoldások alkalmazása általában a munkahelyi teljesítmény értékelésére szolgáló automatizált adatkezelést valósít meg. Így Magyarországon a Nemzeti Adatvédelmi és Információszabadság Hatóság is arra a következtetésre, miszerint a mesterséges intelligencia ügyfélértékelés során történő használata a telefonos ügyfélszolgálati munkavállalókkal kapcsolatos profilalkotáshoz is vezethet. Az eset során ugyanis az adatkezelőként eljáró magyarországi bank MI alapú megoldása kulcsszavak, valamint ügyfélélmény alapján rangsorolta a visszahívásra elégedetlen ügyfeleket, illetve a telefonos ügyfélszolgálati munkavállalók teljesítményét is értékelte, az esetükben is profilalkotást valósítva meg.[53]

Ahogy az a fenti esetből is következik, az MI munkahelyi alkalmazásával különösen megnőhet a munkavállalók fokozott értékelésének kockázata. Erre tekintettel a munkáltatóknak ilyen rendszer alkalmazása esetén – még annak bevezetése előtt – különös gondossággal kell felmérniük az adott rendszer alkalmazásának munkavállalókra gyakorolt lehetséges hatásait, amelyet az érintett munkavállalókkal is ismertetni szükséges, az alkalmazandó logika mellett. Így az érintett munkavállalók is felmérhetik a kapcsolódó kockázatokat, és előre láthatják az esetleges pozitív és negatív hatásokat. Mindemellett azonban a munkáltatótól ilyen esetekben különös súllyal várható el az adatvédelmi követelményeknek való megfelelés és a munkaszervezés alapos összehangolása, és az ezekhez szükséges körű transzparencia biztosítása.

[52] GDPR 4. cikk 4. pontja értelmében profilalkotásnak tekintendő 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*”.

[53] NAIH-85-3/2022 ügyszámú határozat, 24-25. o.

Az Innovációs és Technológiai Minisztérium ÚNKP-21-3 kódszámú Új Nemzeti Kiválóság Programjának a Nemzeti Kutatási, Fejlesztési és Innovációs Alapból finanszírozott szakmai támogatásával készült.

f) Az okosotthonokkal kapcsolatos átlátható adatkezelés

Már a kezdetektől fogva alapigazságnak tekinthető, miszerint az ember otthona idővel a benne lakókhoz idomul. Ízlésünk megjelenik a festésen, a bútorokon, a berendezési tárgyakon és azok elrendezésén. Az okosotthon is ennek megfelelően azt az alapvető emberi igényt szolgálja ki, hogy lakásunk az igényeinkhez igazodjon, amelyeket azonban a technológia segítségével korábban soha nem látott módon és hatékonysággal képes kielégíteni.

Napjaink okosotthonaiban a népszerűnek számító okostévék mellett egyre többször jelennek meg fűtést és világítás szabályozó, valamint a lakás működésével kapcsolatos eseményeket (például: javítás szükségessége, biztonsági probléma) jelző szenzorok.[54] Ezen szenzorok természetesen számos adatot rögzítenek az adott lakásról, valamint ennek kapcsán a lakás, a benne található helyiségek és eszközök használatáról, így még hatékonyabban állhatnak szolgálatunkra, megismerve szokásainkat és igényeinket. Ezen adatok segítségével azonban érthető módon szenzitív információk is nyerhetők az okosotthonok lakóiról, feltérképezhető napirendjük, valamint személyiségprofil is alkotható róluk, amelyet az azt birtokló cégek hatékonyan alkalmazhatnak például személyre szabott marketing ajánlatok elkészítéséhez és eljuttatásához is. Mindez értelemszerűen jelentős behatással járhat az érintett magánéletébe és a személyre szabott tartalmak és szolgáltatások jelentette előnyök mellett hátrányokhoz is vezethet, különösen, ha ezen adatokhoz jogosulatlan személyek férnek hozzá, vagy ha ezen adatokat az érintettek számára átláthatatlan és behatárolhatatlan módon értékesítik.

A fentiekre tekintettel az okosotthonok és a különböző, kapcsolódó okoseszközök fejlesztőitől, gyártóitól, illetve forgalmazóitól és a kapcsolódó szolgáltatások nyújtóitól elvárató, hogy átlátható képet adjanak az általuk folytatott adatkezelésről, különösen ideértve az adott eszköz, valamint a kapcsolódó applikáció, szoftveres megoldás által gyűjtött adatok körét, az esetleges helymeghatározást, valamint

[54] Nathaniel Kunes, How Is Smart Home Technology Shaping The Property Management Industry? Forbes, 2022.03.08, https://www.forbes.com/sites/forbesbusinesscouncil/2022/03/08/how-is-smart-home-technology-shaping-the-property-management-industry/?sh=1458eb0e382c [2022.09.06]

Az Innovációs és Technológiai Minisztérium ÚNKP-21-3 kódszámú Új Nemzeti Kiválóság Programjának a Nemzeti Kutatási, Fejlesztési és Innovációs Alapból finanszírozott szakmai támogatásával készült.

ezen adatok felhasználását (például: személyre szabott marketing üzenetek küldése vagy szolgáltatások nyújtása céljából).

2. Önvezető járművek általi adatkezelés

Az önvezető autók radikális módon alakítják át a közlekedést. A segítségükkel könnyebben elkerülhetők a közúti balesetek, hatékonyabban szervezhető meg a személy- és áruszállítás, csökkenthető a károsanyagkibocsátás, illetve az üzemanyagköltségek. Természetesen azonban a technológia számos kockázatot is hordoz magában, ideértve – a mesterséges intelligencia kapcsán írtakhoz hasonlóan – az okozott balesetekért, károsodásért való felelősség körét, az adatvédelmi és adatbiztonsági kockázatokat, valamint az alkalmazott technológia átláthatóságát, az esetleges negatív következményekre való felkészülést.

Az önvezető technológiát jellemzően 0-5 szintig értékelik, annak figyelembevételével, hogy a technológia mennyire önálló, és milyen mértékben igényli a vezető közreműködését. A 0-2 szintekre jellemzően a vezetést segítő, illetve kiegészítő funkciók jellemzők (például: a balesetek elkerülése érdekében automatikus fékezés, sávtartás figyelése), míg a 3-4. szinten már az adott útszakaszon jellemzően az önvezető technológia végzi a vezetést, és a sofőrnek pusztán szükség esetén kell beavatkoznia. Ezzel szemben az 5. szintre már a teljes automatizáció jellemző, ahol a „hús-vér sofőr" lényegében utassá válik. Hangsúlyozandó, hogy mind az Egyesült Államok, mind az Európai Unió területén a 0-2. szintű önvezető technológia tekinthető csak részlegesen elterjedtnek, míg a 3-5. szintet garantáló technológiai megoldások jellemzően még csak kísérleti szakaszban vannak.[55]

[55] NHTSA, Automated Vehicles for Safety, https://www.nhtsa.gov/technology-innovation/automated-vehicles-safety, 2022.08.18.

Az Innovációs és Technológiai Minisztérium ÚNKP-21-3 kódszámú Új Nemzeti Kiválóság Programjának a Nemzeti Kutatási, Fejlesztési és Innovációs Alapból finanszírozott szakmai támogatásával készült.

3. Drónok általi adatkezelés

A pilóta nélküli légijárművek alatt a Nemzetközi Polgári Repülési Szervezet (ICAO) meghatározása szerint olyan járműveket értünk, amelyek esetén a fedélzeten nem tartózkodik irányítószemélyzet[56]. Ehhez hasonló definíciót alkalmaz a Bizottság (EU) 2019/945 felhatalmazáson alapuló rendelete a pilóta nélküli légijármű-rendszerekről és a pilóta nélküli légijármű-rendszerek harmadik országbeli üzembentartóiról is, amely szerint pilóta nélküli légijármű „*bármely olyan légi jármű, amely a fedélzetén tartózkodó pilóta nélkül üzemel vagy amelyet ilyen üzemmódra terveztek, és amely önálló vagy távirányítással történő üzemelésre képes*”.[57] Megemlítendő továbbá, hogy a pilóta nélküli légijárművekre gyakran használják a „drón” kifejezést is, amely mind a polgári, mind a katonai célból használt eszközökre széleskörben alkalmazott. A drónokat a használóik – akár a közhatalom gyakorlásának keretein belül, akár kereskedelmi vagy magáncélból folytatott repülési műveletek esetén – gyakran szerelik fel kamerával, tekintettel arra, hogy segítségükkel nehezen megközelíthető helyek (például: távközlési berendezések, mezőgazdasági művelés alatt álló vagy építési területek) is könnyen megfigyelhetők, illetve a segítségükkel nagyobb területekről is jó minőségű felvételek készíthetők. A fentiek szerinti drónokkal folytatott adatkezelés esetén kiemelendő azonban, hogy ezen eszközök megfigyelőképességük révén jelentős behatást jelentenek az érintettek magánszférájába, valamint a kapcsolódó adatkezelések során az adatkezelő személye gyakran rejtve marad, hiszen az érintettek sokszor nem is észlelik az adatkezelést, vagy csak magát a drónt.[58] Erre tekintettel szükséges az érintettek proaktív és hatékony tájékoztatása az adatkezelésről, amely az adatkezelés jellemzői és körülményei, valamint az irányadó jogszabályi rendelkezések tükrében különböző formával és tartalommal bírhat. A gyakorlatban megoldás lehet a vonatkozó légiközlekedés kapcsán használt applikáción belül, az üzemeltető honlapján, közösségi médián keresztüli, valamint a helyszínen történő tájékoztatás, a megfigyelt terület megjelölése, a kezelőszemélyzet kiemelése, továbbá mindezek kombinációja, azonban a megfelelő tájékoztatás csak a vonatkozó művelet és kapcsolódó adatkezelés valamennyi körülményének ismeretében alakítható ki.

[56] International Civil Aviation Organization, Remotely Piloted Aircraft System (RPAS) Concept of Operations (CONOPS) for International IFR Operations, https://www.icao.int/safety/UA/Documents/ICAO%20RPAS%20CONOPS.pdf, 2022.08.20. 1.
[57] A Bizottság (EU) 2019/945 felhatalmazáson alapuló rendelete (2019. március 12.) a pilóta nélküli légijármű-rendszerekről és a pilóta nélküli légijármű-rendszerek harmadik országbeli üzembentartóiról, OJ L 152, 11.6.2019, p. 1–40 (BG, ES, CS, DA, DE, ET, EL, EN, FR, HR, IT, LV, LT, HU, MT, NL, PL, PT, RO, SK, SL, FI, SV), 3. cikk 1. pontja.
[58] A Nemzeti Adatvédelmi és Információszabadság ajánlása a drónokkal megvalósított adatkezelésekről, 2014, 10-11. o.

Az Innovációs és Technológiai Minisztérium ÚNKP-21-3 kódszámú Új Nemzeti Kiválóság Programjának a Nemzeti Kutatási, Fejlesztési és Innovációs Alapból finanszírozott szakmai támogatásával készült.

A fentiekre tekintettel a drónok gazdasági vagy rendvédelmi célú alkalmazására a gyakorlatban jellemzően szigorúbb szabályok irányadók, mint a magáncélú felhasználásra, tekintettel arra, hogy ezen alkalmazási módok általában jelentősebb kockázattal bírnak az érintettek magánszférájára és érdekeire nézve. Erre tekintettel a francia adatvédelmi hatóság is a közelmúltban vizsgálta a francia rendvédelmi szervek drónokkal folytatott adatkezelését. Ennek keretében megállapította, hogy a rendvédelmi szervek jogsértő módon jártak el, amikor kamerával felszerelt drónokkal figyelték a koronavírus világjárvány terjedése okán bevezetett kijárási tilalomnak történő megfelelést, a hatóság pedig kötelezte a francia Belügyminisztériumot a fenti gyakorlat megszüntetésére, amelyre a hatóság álláspontja szerint csak megfelelő jogszabályi felhatalmazás alapján lett volna lehetőség.[59]

A kereskedelmi célú felhasználás esetén értelemszerűen enyhébb szabályok alkalmazandók, azonban az adatkezelőnek ez esetben is fokozott gondossággal kell eljárnia a drónnal folytatott művelet és a kapcsolódó adatkezelés során (például: az ott dolgozó személyzet által kevéssé látogatott terület megfigyelése ipari területen), továbbá ugyancsak szükséges az ezekre tekintettel indokolt mértékű tájékoztatást megadni az érintettek részére. Hangsúlyozandó továbbá, hogy az érintettek tájékoztatásának kötelezettsége magáncélú drónnal folytatott adatkezelés esetén is felmerülhet, azonban jóval enyhébb mértékben és szűkebb körben, tekintettel arra, hogy ezen esetben az irányadó adatvédelmi jogszabályok sem feltétlenül alkalmazandók az adatkezelő magáncélú vagy családi körben folytatott adatkezeléseire.

4. Egészségügy és technológia

Az egészségügyi szolgáltatások adatvédelmi aspektusai különös figyelmet érdemelnek, tekintettel arra, hogy az egészségügyi szolgáltatások, valamint az egészségügyi rendszer szereplőinek tevékenysége kiemelt társadalmi hatásokkal bír, az ez által érintett, gyakran szenzitív helyzetben lévő személyeknek

[59] A francia adatvédelmi hatóság („*La Commission nationale de l'informatique et des libertés*"; „**CNIL**") SAN-2021-003 számú, 2021. január 21-én kelt határozata, https://www.legifrance.gouv.fr/cnil/id/CNILTEXT000042960768 [2022.08.29]

Az Innovációs és Technológiai Minisztérium ÚNKP-21-3 kódszámú Új Nemzeti Kiválóság Programjának a Nemzeti Kutatási, Fejlesztési és Innovációs Alapból finanszírozott szakmai támogatásával készült.

(különösen ideértve a betegeket) pedig jelentős érdekük fűződik ahhoz, hogy a személyes adataik kezelését megfelelő módon áttekinthessék, annak hatásait megérthessék.

Mindez sok szempontból összekapcsolódik a betegeket az egészségügyi szolgáltatások igénybevétele keretében megillető betegjogokkal, valamint az ezen szolgáltatások és kapcsolódó tevékenységek sajátosságaival. Így értelemszerűen egy kórházi beteget – állapota, illetve körülményei figyelembevételével – megilleti a tájékozott döntés joga az őt érintő beavatkozások kapcsán, ehhez kapcsolódóan pedig jogosult arra is, hogy a személyes adatainak kórház általi kezelését megismerhesse, áttekinthesse, és azzal kapcsolatban is döntéseket hozhasson (ideértve például az egészségügyi dokumentáció megtekintését, az arról történő másolatkérést).

A fenti jogok gyakorlása, valamint az érintettek tájékoztatásának kötelezettsége azonban sokszor sajátságosan alakul az egészségügy területén is egyre inkább elterjedő mesterséges intelligencia alapú és egyéb modern technológiával kapcsolatos megoldások területén. Ennek körében kiemelendő az egészségügyi robotok megjelenése, amelyek számos feladatot képesek ellátni, az egyszerűbb feladatoktól a betegek ápolásán és gondozásán át a komplexebb egészségügyi beavatkozásokban történő közreműködésig. Így például 2021-ben a Los Angeles-i Cedars Sinai kórházban bevezették a Moxi nevű robotot, akit az ápolók telefonon keresztül is igénybe vehetnek egy-egy feladat elvégzéséhez. A robot az eddigi tapasztalatok alapján gyors és hatékony segítséget képes nyújtani az egészségügyi személyzet számára, valamint folyamatos visszajelzést tud küldeni az aktuális állapotáról.[60] A Hanson Robotics nevű hong kong-i társaság által kifejezetten a betegekkel való interakciók céljára fejlesztett Grace nevű ápolórobot már ennél is többre képes, így számos szenzorral felszerelten képes például ellenőrizni a betegek testhőmérsékletét és pulzusát, valamint több nyelven is társalogni velük.[61]

[60] Robots Help Nurses Get the Job Done–With Smiles and Beeps, Cedars Sinai, 2021.11.29, https://www.cedars-sinai.org/newsroom/robots-help-nurses-get-the-job-donewith-smiles-and-beeps/ [2022.08.30]
[61] Rebecca Cairns, Meet Grace, the ultra-lifelike nurse robot, CNN, 2021.08.19, https://edition.cnn.com/2021/08/19/asia/grace-hanson-robotics-android-nurse-hnk-spc-intl/index.html [2022.08.30]

Az Innovációs és Technológiai Minisztérium ÚNKP-21-3 kódszámú Új Nemzeti Kiválóság Programjának a Nemzeti Kutatási, Fejlesztési és Innovációs Alapból finanszírozott szakmai támogatásával készült.

A fenti kiszolgáló, ápoló- és egyéb egészségügyi robotok általi adatkezelés kétségkívül képes a betegápolás színvonalának, valamint a kórházüzemeltetés hatékonyságának javítására, az eredmények révén pedig a betegek egészségügyi problémái előre jelezhetők, a terápia hatékonysága sok esetben növelhető. Ugyanakkor az sem hagyható figyelmen kívül, hogy a betegek jellemzően kiszolgáltatott helyzetben vannak, és kevésbé képesek jogaik aktív gyakorlására, így például még kevesebb lehetőséggel bírnak arra, hogy egészségügyi és más személyes adataik elemzését, kiértékelését átláthassák, azzal kapcsolatban jogaikat érvényesíthessék (például: hozzáférhessenek ezen adataikhoz, vagy kérjék azok továbbítását egy további egészségügyi szolgáltató részére). Erre tekintettel a hasonló megoldások alkalmazóinak különös gondot kell fordítania arra, hogy adatkezeléseiket a betegek számára átláthatóvá tegyék, valamint a jogaik gyakorlását megkönnyítsék. Így a beteg egészségügyi adatainak kezeléséről való tájékoztatásra sor kerülhet például a robotnak a beteggel történő interakciója során, ahol a robot szóban tájékoztatást adhat, azt egy képernyőn megjelenítheti, valamint az érintett jogainak gyakorlása esetén a kérelmét maga is teljesítheti, vagy azt a kórház egy erre kijelölt szakemberének továbbíthatja.

5. A blockchain és az adatkezelés

A blockchain egy megosztott és megváltoztathatatlan főkönyvként írható le, amelyen keresztül tranzakciók rögzíthetők.[62] A blockchain technológia elsősorban a kriptovaluta piac területén terjedt el, azonban más esetekben is használható, ideértve ellátási láncolatok rögzítését, nyomon követését. Így például a VinAssure nevű amerikai blockchain alapú platform segítségével az Európában előállított borok ellátási láncolata, biztonsági és minőségi kiszolgálása ellenőrizhető.[63]

A blockchain technológia a fentiekre tekintettel sok szempontból forradalmasítja a pénzügyi piacokat, valamint az elszámoláshoz, különböző tranzakciók rögzítéséhez és nyomon követéséhez használt rendszereket, tekintettel arra, hogy ennek révén növelhető az egyes tranzakciós láncolatok és

[62] What is blockchain technology? IBM, https://www.ibm.com/topics/what-is-blockchain [2022.08.30]
[63] Research leading blockchain use cases, IBM, https://www.ibm.com/blockchain/use-cases/ [2022.08.30]

Az Innovációs és Technológiai Minisztérium ÚNKP-21-3 kódszámú Új Nemzeti Kiválóság Programjának a Nemzeti Kutatási, Fejlesztési és Innovációs Alapból finanszírozott szakmai támogatásával készült.

nyilvántartások átláthatósága, azok biztonsága, valamint kiiktathatók az elszámoláshoz, nyilvántartáshoz használt közvetítő szolgáltatók. A fentieken túl azonban a blockchain technológia alkalmazása személyes adatokat is érinthet, ideértve a résztvevőket azonosító publikus kulcsokat, valamint a tranzakciókon belül „helyet foglaló" egyes adatokat (például: az egyes blokkokban rögzített személyes adatokat).[64] Ennek kapcsán a tájékoztatás követelménye ugyanúgy kell, hogy érvényesüljön mint más adatkezelések esetén, az adatkezelés által érintett személyeket pedig az irányadó jogszabályok szerint szükséges tájékoztatni személyes adataik kezeléséről (ideértve például a tranzakcióra vonatkozó kapcsolattartás kezdetekor vagy az annak során hivatkozott weboldalon elérhető adatvédelmi tájékoztatón keresztül).

Megemlítendő ugyanakkor, hogy a tájékoztatás kapcsán írtak mellett a blockchain technológia egyes érintetti jogok gyakorlása esetén további jelentős kihívásokat tartogat, ideértve különösen a törléshez való jogot, amely érthető módon az adatok teljes és végleges törlése révén nem gyakorolható, hiszen ez magának a tranzakciós láncolatnak a megmásíthatatlanságát sértené; ennek érdekében, ha a tranzakcióhoz kapcsolódó adat kezelésére már nincs szükség – a francia adatvédelmi hatóság által kiemeltek szerint – megoldás lehet az adott információ elérhetetlenné tétele (például: megfelelő algoritmusok alkalmazásával), így a tranzakciók láncolata sem sérül, és az érintetti jog gyakorlása is helyet foghat.[65]

A fentiekre tekintettel a blockchain technológia alkalmazása esetén a tájékoztatásnak különös gonddal kell kitérnie az érintetti jogok érvényesíthetőségének technikai lépéseire, tekintettel arra, hogy ezen közérthetően átadott ismeretek nélkül az érintett nem lehet képes arra, hogy adatvédelmi jogait megfelelően gyakorolja. Ehhez kapcsolódóan továbbá a vonatkozó adatvédelmi tájékoztató közlése is a technológia és a vonatkozó szerződéses vagy egyéb kapcsolat sajátosságaihoz kell, hogy idomuljon, így javasoltan a tájékoztatás közlésének az érintettel való kapcsolattartás keretén belül vagy olyan felületen

[64] CNIL, Blockchain and the GDPR: Solutions for a responsible use of the blockchain in the context of personal data, 2018.11.06, https://www.cnil.fr/en/blockchain-and-gdpr-solutions-responsible-use-blockchain-context-personal-data
[65] CNIL, Blockchain. Solutions for a responsible use of the blockchain in the context of personal data (https://www.cnil.fr/en/blockchain-and-gdpr-solutions-responsible-use-blockchain-context-personal-data), 8. o.

Az Innovációs és Technológiai Minisztérium ÚNKP-21-3 kódszámú Új Nemzeti Kiválóság Programjának a Nemzeti Kutatási, Fejlesztési és Innovációs Alapból finanszírozott szakmai támogatásával készült.

kell megvalósulnia, amiről logikusan feltételezhető, hogy az érintettek látogatni fogják és könnyen elérhetik.

6. A virtuális valóság, a kiterjesztett valóság és a metaverzum adatvédelmi szempontjai

Virtuális valóság (VR) alatt olyan komputer által generált virtuális környezetet értünk, amely körbeveszi a felhasználót, és reagál annak cselekvéseire.[66] A virtuális valóság számos területen használható, ideértve például a kreatív tartalomgyártás és kommunikáció területét, a szakképzési tevékenységet (például: pilóták képzését), valamint tervezésre és háromdimenziós tárgyak megjelenítésére.[67] A fentieken túl a VR technológia kiemelten használható a videójátékipar területén is. Például a Meta által gyártott Meta Quest 2 VR sisak és felszerelés segítségével is számos játék és egyéb tartalom érhető el.[68]

A VR mellett ugyancsak említést érdemel a kiterjesztett valóság (AR), amely lényegében a virtuális valóságot és a való világot „gyúrja egybe", virtuális elemeket (például: képek, hangok, videótartalmak) integrálva az utóbbiba.[69] Az AR technológia a VR-hez hasonlóan szintén egyre inkább elterjedté vált, az utóbbi években pedig kifejezetten a játék applikációk területén vált közismertté. E körben említést érdemel a 2016-ban megjelenő Pokémon Go játék[70], amelynek segítségével az okostelefon tulajdonosa az applikáció telepítését követően a való világban kereshet virtuálisan megjelenített Pokémon szörnyeket. Természetesen az AR széleskörű lehetőségeket rejt magában a videójátékok piacán túl a marketing, valamint az online szolgáltatások számos területén, segítségével továbbá az ipari tervezési folyamatok hatékonyabbá tehetők, az ügyfélélmény növelhető. Az AR képes lehet továbbá az oktatást is forradalmasítani, hiszen segítségével a tananyag a tankönyvek lapjairól a való világba „költöztethető".

[66] Virtual Reality (VR), Gartner Glossary, https://www.gartner.com/en/information-technology/glossary/vr-virtual-reality [2022.08.30]
[67] Hilda Clune, Three use cases for virtual reality in enterprise, PwC Australia, Digital Pulse, 2017.05.26, https://www.pwc.com.au/digitalpulse/three-use-cases-virtual-reality-enterprise.html [2022.08.30]
[68] Meta, https://store.facebook.com/quest/products/quest-2 [2022.08.30]
[69] Augmented Reality (AR), Gartner Glossary, https://www.gartner.com/en/information-technology/glossary/augmented-reality-ar [2022.08.30]
[70] Pokémon Go, https://pokemongolive.com/ [2022.08.30]

Az Innovációs és Technológiai Minisztérium ÚNKP-21-3 kódszámú Új Nemzeti Kiválóság Programjának a Nemzeti Kutatási, Fejlesztési és Innovációs Alapból finanszírozott szakmai támogatásával készült.

Így például a Froggipedia[71] elnevezésű applikáció segít megérteni a békák életmódját és felépítését, míg a WWF (World Wildlife Fund) WWF Free Rivers elnevezésű applikációja a folyók működését mutatja be[72]. A fentiekhez hasonló applikációk a jövőben jelentős segítséget nyújthatnak az oktatás és az ismeretterjesztés területén, valamint alkalmasak lehetnek arra, hogy egy-egy területről vagy kérdéskörről bővebb, emészthető információkat nyújtsanak az érdeklődőknek.

A fentiekre tekintettel kétségtelennek tűnik, hogy a VR és az AR alkalmazása számos előnnyel kecsegtet, azonban alkalmazásukkal adatvédelmi aggályok is felmerülnek, tekintve, hogy a segítségükkel jelentős mértékben elemezhetők a felhasználók szokásai, fizikai és mentális állapota, környezete, az így gyűjtött információk pedig könnyen alkalmazhatók profilalkotás céljára és személyre szabott marketing vagy egyéb üzenetek küldésére, adott esetben szenzitív kategóriába tartozó felhasználók (különösen: gyermekek) befolyásolására. Erre tekintettel különösen fontos etikus és átlátható adatkezelési gyakorlat kialakítása és ennek következetes érvényesítése. Természetesen nem cél, hogy az adatvédelmi megfelelés a felhasználói élményt ellehetetlenítse vagy a felhasználókkal való interakciónak észszerűtlenül gátat szabjon, azonban elvárható a hasonló alkalmazások fejlesztőitől, valamint az azokat a felhasználók részére biztosító szolgáltatóktól, hogy a személyes adatok gyűjtésére és az adatkezelés céljaira az érintettek figyelmét felhívják, valamint az érintettek adatvédelmi jogainak gyakorlását biztosítják (például adott esetben a marketing tartalmak megjelenítésével és a kapcsolódó adatkezeléssel szembeni tiltakozást). A tájékoztatásra sor kerülhet a „hagyományos” módok (például: az adatvédelmi tájékoztató szolgáltatói weboldalon, illetve a vonatkozó áruházban, applikáción keresztül történő közzététele) mellett akár egyes információk virtuális térben való megjelenítése, valamint az érintetti jogok gyakorlásának ezen keretek közt történő lehetővé tétele útján (például: az adott virtuális valóságban egy szöveg törlése, tárgy elpusztítása a vonatkozó személyes adatok törlése iránti igényt is jelentheti). Ezzel kapcsolatban azonban általánosan elterjedt iparági gyakorlatok még nem alakultak ki, ez vélhetőleg a következő évek feladata lesz majd.

[71] Froggipedia, https://apps.apple.com/us/app/froggipedia/id1348306157 [2022.08.30]
[72] WWF Free Rivers, https://apps.apple.com/us/app/wwf-free-rivers/id1349935575 [2022.08.30]

Az Innovációs és Technológiai Minisztérium ÚNKP-21-3 kódszámú Új Nemzeti Kiválóság Programjának a Nemzeti Kutatási, Fejlesztési és Innovációs Alapból finanszírozott szakmai támogatásával készült.

Az AR és a VR mellett érdemes megemlíteni a metaverzumot, amely az adatvédelmi megfontolásokon túl egy sor jogterület, illetve jogi probléma újragondolását teszi szükségessé. A metaverzum kifejezésre vagy jelenségre többféle definíció is ismert[73], jelentős részben azonban a metaverzum egy komplex digitális világként fogható fel, amelyen belül számos interakció, valamint tranzakció végezhető (például: digitálisan létező ingatlanok és tárgyak adása, vétele). Érdekes kérdésnek tekinthető, hogy egy ilyen digitális világban milyen módon érvényesülhet a személyes adatok védelme. Vélhetőleg eleve akkor alkalmazhatók az adatvédelmi szabályok, amennyiben az ezen világban megjelenő karakterek vagy avatárok azonosítják a „hús-vér" felhasználót (például: nevük, megjelenésük révén) vagy ha ezek tevékenysége kapcsán olyan információ válik elérhetővé, amely a felhasználót azonosítja (például: személyes tárgyak, környezet digitális formában való megjelenítése). Ilyen esetben az adatkezelőket a személyes adatok kezelése és az érintettek erről való tájékoztatása, illetve az érintetti jogok gyakorlásának támogatása kapcsán a felelősség elsősorban az adott digitális világot működtető szervezetet terheli, amely azt, valamint a felhasználókhoz kapcsolódó adatokat nyilván tartja, kezeli. Adott esetben azonban adatkezelőnek minősülhetnek további felhasználók is, ha a fentiek szerint képesek lehetnek arra, hogy más felhasználókat azonosítsanak. Az ezzel kapcsolatos adatvédelmi szempontok és esetleges jogi kötelezettségek részletes elemzése azonban túlmutat ezen tanulmány keretein, így a fenti kérdések megválaszolása a jövő adatvédelmi gyakorlatának feladata lesz.

7. Az arcfelismerő rendszerek alkalmazása és a közbiztonság

Az arcfelismerő rendszerek kiemelt módon képesek hozzájárulni a közbiztonság erősödéséhez, valamint a súlyos bűncselekmények gyanúsítottjainak könnyebb azonosításához. Alkalmazásuk azonban alkotmányjogi, illetve emberi jogi szempontból is számos esetben megkérdőjelezhető. Ennek okai közé sorolható ezen rendszerek esetleges társadalomtorzító hatása, polgári demokráciákra gyakorolt veszélyei, a megfigyelt személyek magánéletébe való jelentős behatás, valamint a rendszerek pontatlanságával, az esetleges diszkriminációval kapcsolatos kifogások is. Ez egybevágni látszik továbbá

[73] Lásd például: Cathy Hackl, Defining The Metaverse Today, 2021.05.02, https://www.forbes.com/sites/cathyhackl/2021/05/02/defining-the-metaverse-today/?sh=50bfe19c6448 [2022.08.30]

Az Innovációs és Technológiai Minisztérium ÚNKP-21-3 kódszámú Új Nemzeti Kiválóság Programjának a Nemzeti Kutatási, Fejlesztési és Innovációs Alapból finanszírozott szakmai támogatásával készült.

az arcfelismerő rendszerek európai alkalmazásával kapcsolatos bírósági és adatvédelmi hatósági gyakorlattal. Egy marseille-i bíróság például 2020-ban egy arcfelismerő rendszer iskolai használatát tilalmazó döntést hozott[74], egy évvel korábban pedig a francia adatvédelmi hatóság is akként foglalt állást, hogy gimnáziumok területén nem alkalmazhatók arcfelismerő rendszerek.[75]

A fentiek okán az Európai Adatvédelmi Testület és az Európai Adatvédelmi Biztos is kiemelte közös véleményében is kifejezett felhívást intézett az arcfelismerő rendszerek közterületen való automatizált felhasználására, valamint ezzel összefüggésben az MI online térben való széleskörű távoli azonosítására.[76] Ezzel összhangban a Mesterséges Intelligenciáról szóló Jogszabály tervezet is tilalmazza „valós idejű" távoli biometrikus azonosító rendszerek használata nyilvános helyeken bűnüldözési célokból, kivéve, ha az ilyen használat feltétlenül szükséges (i) a bűncselekmények konkrét potenciális áldozatainak célzott felkutatása (ideértve eltűnt gyermekeket is), (ii) természetes személyek életét vagy fizikai biztonságát fenyegető konkrét, jelentős és közvetlen veszély, illetve terrortámadás megelőzése, valamint (iii) az érintett tagállam joga szerint legalább három évi szabadságvesztéssel vagy szabadságelvonással járó intézkedéssel büntetendő bűncselekmények elkövetőinek elfogása érdekében.[77] A fentiek kapcsán hangsúlyozandó, hogy a tervezet a „valós idejű" távoli biometrikus azonosító rendszerek alatt olyan rendszerek alkalmazását érti, ahol „*a biometrikus adatok rögzítése, összehasonlítása és azonosítása azonnal, majdnem azonnal vagy mindenesetre jelentős késleltetés nélkül történik*", e körben pedig szigorúbb követelményeket támaszt mint a „nem valós idejű" távoli biometrikus azonosító rendszerek esetén, ahol „*a biometrikus adatokat már rögzítették, és az összevetésre és az azonosításra csak jelentős késleltetéssel kerül sor*".[78] Megemlítendő azonban, hogy a tervezet mind a „valós idejű", mind a „nem valós idejű" távoli biometrikus azonosító rendszereket nagy kockázatúnak minősíti, tekintettel arra, hogy „*természetes személyek távoli biometrikus azonosítására szolgáló MI-rendszerek technikai pontatlansága torzított eredményekhez vezethet, és diszkriminatív hatásokat eredményezhet*", amely

[74] Tribunal Administratif de Marseille, N° 1901249, https://www.laquadrature.net/wp-content/uploads/sites/8/2020/02/1090394890_1901249.pdf [2022.09.07]
[75] CNIL Expérimentation de la reconnaissance faciale dans deux lycées : la CNIL précise sa position, 2019.10.29, https://www.cnil.fr/fr/experimentation-de-la-reconnaissance-faciale-dans-deux-lycees-la-cnil-precise-sa-position [2022.09.07]
[76] Az Európai Adatvédelmi Testület és az Európai Adatvédelmi Biztos 5/2021. sz. közös véleménye a mesterséges intelligenciára vonatkozó harmonizált szabályok (a mesterséges intelligenciáról szóló jogszabály) megállapításáról szóló európai parlamenti és tanácsi rendeletre irányuló javaslatról, 11-12. o.
[77] Mesterséges Intelligenciáról szóló Jogszabály tervezet 5. cikk (1) d) pontja.
[78] Mesterséges Intelligenciáról szóló Jogszabály tervezet (8) preambulum-bekezdése.

Az Innovációs és Technológiai Minisztérium ÚNKP-21-3 kódszámú Új Nemzeti Kiválóság Programjának a Nemzeti Kutatási, Fejlesztési és Innovációs Alapból finanszírozott szakmai támogatásával készült.

„különösen releváns az életkor, az etnikai hovatartozás, a nem vagy a fogyatékosságok tekintetében". Erre tekintettel a tervezet értelmében a távoli biometrikus azonosító rendszerek mindkét fenti típusára naplózási képességekkel és emberi felügyelettel kapcsolatos különös követelmények kell, hogy vonatkozzanak.[79]

A Mesterséges Intelligenciáról szóló Jogszabály tervezet a fentieken túl a „valós idejű" távoli biometrikus azonosító rendszerek vonatkozásában kiemeli továbbá, miszerint a „valós idejű" távoli biometrikus azonosító rendszerek nyilvánosság számára hozzáférhető helyeken, bűnüldözés céljából történő használata esetén a használatnak meg kell felelnie a szükséges és arányos biztosítékoknak és feltételeknek, különösen ideértve az időbeli, földrajzi és személyi korlátozásokat.[80] Ezen korlátozások, valamint általánosságban az adott rendszer esetleges hatásainak, adatvédelmi megfelelésének felmérésében, értékelésében jelentős segítséget jelenthet a vonatkozó rendszer előzetes tesztelése, erre meghatározott, kevés személy által látogatott területen, adott esetben több periódusban. Az ezen tesztelések során nyert tapasztalatokat az adatkezelő rögzítheti, hatásvizsgálati dokumentációba foglalhatja, egy esetleges hatósági ellenőrzés vagy az érintett panasza esetén pedig a fenti megfelelés alátámasztásához is használhatja.[81]

Mindemellett a tervezet kiemeli, hogy a „valós idejű" távoli biometrikus azonosító rendszerek fentiek szerinti alkalmazása esetén minden egyes használat – kellően indokolt sürgős helyzet kivételével – az illetékes igazságügyi vagy független közigazgatási hatóság által előzetesen adott engedélyhez kell, hogy kötött legyen, amely csak indokolt megkeresésre bocsátható ki.[82] A fentiek szerinti kellően indokolt sürgős esetek alatt a gyakorlatban olyan helyzetek érthetők, *„amikor a szóban forgó rendszerek használatának szükségessége ténylegesen és objektíve lehetetlenné teszi az engedély megszerzését a használat megkezdése előtt*"; az ilyen helyzetekben a rendszer használata a minimálisra kell, hogy

[79] Mesterséges Intelligenciáról szóló Jogszabály tervezet (33) preambulum-bekezdése.
[80] Mesterséges Intelligenciáról szóló Jogszabály tervezet 5. cikk (2) bek. E körben a tervezet (20) preambulum-bekezdése is kiemeli, miszerint a megfelelő időbeli és térbeli korlátozások közé sorolandók különösen a fenyegetésekkel, az áldozatokkal vagy az elkövetőkkel kapcsolatos bizonyítékok vagy jelzések.
[81] Necz Dániel, A mesterséges intelligencia belügyi és biztonsági célú alkalmazása, Scientia et Securitas, 2020, 1/1, 51.
[82] Mesterséges Intelligenciáról szóló Jogszabály tervezet 5. cikk (3) bek.

Az Innovációs és Technológiai Minisztérium ÚNKP-21-3 kódszámú Új Nemzeti Kiválóság Programjának a Nemzeti Kutatási, Fejlesztési és Innovációs Alapból finanszírozott szakmai támogatásával készült.

korlátozódjon, az engedély későbbi beszerzése esetén pedig az illetékes bűnüldöző hatóságnak meg kell indokolnia, hogy az adott esetben miért nem volt lehetősége arra, hogy az engedélyt korábban megkérje.[83]

A fentieken túl az Európai Adatvédelmi Testület az arcfelismerő technológia bűnüldözési területen való alkalmazásáról szóló 2022/05. sz. iránymutatása is részletesen áttekinti az arcfelismerő rendszerek alkalmazásának adatvédelmi szempontjait, többek között az ún. bűnügyi adatvédelmi irányelv[84] rendelkezéseivel is összhangban. Az állásfoglalás ennek tükrében kiemeli, miszerint biometrikus adatkezelést megelőzően az adott nyomozáshoz szükséges felvételek törlendők vagy anonimizálandók (például: elhomályosítás útján, a visszaállítás lehetősége nélkül)[85]. Az iránymutatás kitér továbbá a tájékoztatás követelményére is, amely teljesíthető – többek között – az adatkezelő weboldalán, nyomtatott formában vagy egyéb, az érintett számára könnyen hozzáférhető módon.[86] Természetesen azonban a tájékoztatás nem kizárólag ezen megoldások útján teljesíthető, így az eset körülményei tükrében vizsgálandó, hogy az érintettek tájékoztatása hogyan valósulhat meg hatékonyan és egyben arányosan.

8. LegalTech megoldások

A LegalTech vagy legal technology olyan innovatív jogi technológiákat és megoldásokat foglal magában, amelyek növelik a jogi szolgáltatások hatékonyságát, valamint támogatják a jogi szolgáltatókat, és segítenek hatékonyabban kielégíteni az ügyfelek igényeit. A LegalTech megoldások közé sorolhatók –

[83] Mesterséges Intelligenciáról szóló Jogszabály tervezet (21) preambulum-bekezdése.
[84] 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, OJ L 119, 4.5.2016, p. 89–131 (BG, ES, CS, DA, DE, ET, EL, EN, FR, HR, IT, LV, LT, HU, MT, NL, PL, PT, RO, SK, SL, FI, SV)
[85] az Európai Adatvédelmi Testület 2022.05.12-én elfogadott, az arcfelismerő technológia bűnüldözési területen való alkalmazásáról szóló 2022/05. sz. iránymutatása, 21-22. o.
[86] Uo. 21. o.

Az Innovációs és Technológiai Minisztérium ÚNKP-21-3 kódszámú Új Nemzeti Kiválóság Programjának a Nemzeti Kutatási, Fejlesztési és Innovációs Alapból finanszírozott szakmai támogatásával készült.

többek között – a különböző szerződéskezelő, valamint dokumentum felülvizsgálattal, kutatással és adatbányászattal kapcsolatos, elemzések végzésére használt, valamint a jogi chatbot megoldások.

Ezen utóbbi megoldások közé tartozik például a „robot ügyvédként" is aposztrofált DoNotPay nevű jogi chatbot[87], amely kevésbé komplikált jogi ügyeket is képes elintézni, ideértve parkolási bírságokkal kapcsolatos jogorvoslat benyújtását, valamint egyszerűbb ügyintézésben is segítséget nyújt (például: előfizetéseket mond le). Az ilyen megoldások többféle előnyt is kínálnak a fogyasztók számára, ideértve például az ügyvédi munkadíjaknál alacsonyabb díjakat, a rugalmasságot ígérő ügyintézést. Azonban értelemszerűen az előnyök mellé hátrányok sora is társul, ideértve különösen a „hús-vér" ügyvédi felügyelet nélküli ügykezelést, valamint az esetleges műhibáért való felelősség tisztázatlanságát. A fentiek mellett ugyancsak kiemelendők a chatbot megoldások alkalmazásával kapcsolatos adatvédelmi szempontok, ezek figyelembevétele hiányában ugyanis az érintettek nem rendelkezhetnek kellő ismerettel arról, hogy az adataik az ügykezelésen kívül egyéb célból is felhasználásra kerülhetnek-e, és ha igen, arra hogyan is kerül sor. Így a személyes adatok kezeléséről való tájékoztatást (ideértve az adatkezelés legfontosabb jellemzőinek összefoglalását, illetve az adatvédelmi tájékoztató elérhetőségére való utalást) szükséges a chabottal folytatott kommunikációba beépíteni, hogy az érintett kellő információ birtokában dönthessen arról, hogy a chatbot megoldás által nyújtott szolgáltatásokat, támogatást igénybe kívánja-e venni.

Természetesen a chatbot megoldások mellett a dokumentum automatizációval kapcsolatos megoldások is egyre elterjedtebbnek számítanak. Esetükben az adatvédelmi szempontok mellett szintén kiemelendők a felelősséggel kapcsolatos, valamint az etikai szempontok, tekintettel arra, hogy a fenti „robot ügyvéd" megoldásokhoz hasonlóan a gép végez ügyvédi munkát, amelyet nem feltétlenül kíséri megfelelő felügyelet. Mindezen aggályokra tekintettel az Egyesült Államokban például az észak-karolinai ügyvédi

[87] https://donotpay.com/ [2022.09.06.]

Az Innovációs és Technológiai Minisztérium ÚNKP-21-3 kódszámú Új Nemzeti Kiválóság Programjának a Nemzeti Kutatási, Fejlesztési és Innovációs Alapból finanszírozott szakmai támogatásával készült.

kamara folytatott több éves jogvitát a LegalZoom elnevezésű LegalTech szolgáltatóval, amely a fogyasztók érdekeit védő intézkedések bevezetésére vonatkozó megegyezéssel zárult.[88]

A LegalTech története azonban ezzel még közel sem tekinthető lezártnak, figyelemmel arra, hogy a fenti megoldások még a közeljövőben is számos lehetőséget tartogatnak, ideértve többek között a szövegfelismeréssel és analitikai feladatok elvégzésével kapcsolatos megoldásokat, amelyek egyre komplexebb és terjedelmesebb szövegek, dokumentum-halmazok áttekintésére képesek, akár ritkábban használt nyelveken is meghatározott kulcsszavakra keresve.

[88] Joan Rogers, N.C. Law Regulates LegalZoom, Other Legal Doc Providers, Bloomberg Law, 2016.07.26, https://news.bloomberglaw.com/business-and-practice/n-c-law-regulates-legalzoom-other-legal-doc-providers [2022.09.06]

Az Innovációs és Technológiai Minisztérium ÚNKP-21-3 kódszámú Új Nemzeti Kiválóság Programjának a Nemzeti Kutatási, Fejlesztési és Innovációs Alapból finanszírozott szakmai támogatásával készült.

VI. Záró gondolatok

A fentiekre tekintettel tehát megállapítható, miszerint az adatkezelésről való tájékoztatás új technológiai környezetben való alkalmazhatósága kapcsán számos kérdés merül fel, amelyek napjainkban még csak részben válaszolhatóak meg. Ennek tükrében a gyakorlatban számos esetben kérdéses lehet, hogy az adott technológiai megoldással történő adatkezelésről való tájékoztatás megfelelően érthető-e az érintettek számára, valamint, hogy az az érintettek részére tényleges hozzáadott értéket képvisel-e anélkül, hogy az adott technológia hatékony felhasználásának, kiaknázásának a rovására menne, vagy az érintettek döntési kompetenciáját, viselkedését hátrányosan érintené.

Ugyancsak kérdésként merül fel e körben az adott technológia szabályozásának szükségessége, valamint a vonatkozó tájékoztatás mértékének, tartalmának helyes meghatározása, a kapcsolódó sajátos szempontok figyelembevétele. Ennek kapcsán különös hangsúlyt élveznek a vonatkozó technológia, illetve szakterület sajátosságai és az azokra jellemző szakmai és etikai szabályok, jó gyakorlatok is.

Különös hangsúlyt érdemel továbbá a technológiai környezetben történő adatkezelés kapcsán a mesterséges intelligencia szabályozása, amely napjainkban különös kihívást jelent mind a jogalkotó, mind az azt alkalmazó szakemberek számára, így e körben kiemelten fontos az érintettek tájékoztatása az MI által történő döntéshozatalról, az alkalmazott logikáról, és annak hatásairól, a kapcsolódó kockázatok köréről.

Megemlítendő továbbá, hogy mind az Egyesült Államok, mind az Európai Unió joga sok esetben eltérő megközelítést alkalmaz a technológiai környezetben folytatott adatkezelések szabályozására, valamint az ezzel kapcsolatos átláthatóság megteremtése tekintetében. Az amerikai szabályozási törekvések elsődlegesen táptalajt igyekeznek kínálni a technológiai fejlődésnek, és főként az MI általi diszkrimináció, valamint annak a demokratikus társadalmakra kiemelten káros hatásai ellen kívánnak

Az Innovációs és Technológiai Minisztérium ÚNKP-21-3 kódszámú Új Nemzeti Kiválóság Programjának a Nemzeti Kutatási, Fejlesztési és Innovációs Alapból finanszírozott szakmai támogatásával készült.

aktívabban fellépni. Ezzel szemben a kialakulóban lévő európai szabályozás ugyancsak hangsúlyt helyez a technológia pozitív hatásainak kiaknázásra, ugyanakkor rétegzettebb szabályozást igyekszik kialakítani, az egyes MI-rendszerek, valamint kapcsolódó alkalmazási módok sajátos körülményeit és azok hatásait, a vonatkozó kockázatok körét is figyelembe véve, illetve az egyes követelményeket és tilalmakat ezek mértén felállítva.

Természetesen a fenti meglátások egy még gyermekéveit taposó szabályozási környezetről, valamint az ahhoz kapcsolódó adatvédemi, illetve átláthatósággal kapcsolatos követelményekről és szempontokról adnak látképet, azonban számos olyan további szempont is felmerülhet még ezek kapcsán, amelyekre napjainkban talán még nem is gondolunk. A fentiekre tekintettel az elkövetkezendő évek jelentős kihívásokat jelentenek majd az egyes technológiák adatvédelmi megítélése kapcsán. Erre tekintettel azonban a személyes adatok kezeléséről való tájékoztatás követelményének is rugalmasan kell alkalmazkodnia az adott technológia és a társadalmi, valamint a gazdasági környezet változásához, fejlődéséhez, annak érdekében, hogy az érintettek jogai arányos védelemben részesülhessenek.

Az Innovációs és Technológiai Minisztérium ÚNKP-21-3 kódszámú Új Nemzeti Kiválóság Programjának a Nemzeti Kutatási, Fejlesztési és Innovációs Alapból finanszírozott szakmai támogatásával készült.

Felhasznált könyvfejezetek, tanulmányok, folyóiratcikkek

- Danielle Keats Citron, The Roots of Sexual Privacy: Warren and Brandeis & the Privacy of Intimate Life, The Columbia journal of law and the arts, 42/3, 2019
- Eric Barendt: A tudomány szabadsága és a jog. Összehasonlító tanulmány (ford. Csertő István), Budapest, 2017 (az alábbi mű alapján: Academic Freedom and the Law – A Comparative Study. Hart Publishing, Oxford and Portland, Oregon, 2010)
- Klein Tamás, Tóth András (szerk.): Technológia jog – Robotjog – Cyberjog, Wolters Kluwer Hungary, Budapest, 2018
- Monroe E. Price, Stefaan G. Verhulst, Libby Morgan (szerk.): Routledge Handbook of Media Law, Routledge, Oxford, New York, 2013
- Mráz Attila, Deepfake, demokrácia, kampány, szólásszabadság, 249-277. o. In: Török Bernát, Ződi Zsolt (szerk.), A mesterséges intelligencia szabályozási kihívásai, Ludovika Egyetemi Kiadó, Budapest, 2021
- Necz Dániel, A mesterséges intelligencia hatása a szerzői jogra, Iparjogvédelmi és Szerzői Jogi Szemle, 2018/6
- Necz Dániel, A mesterséges intelligencia belügyi és biztonsági célú alkalmazása, Scientia et Securitas, 2020, 1/1
- Paul Bernal, Internet privacy rights: rights to protect autonomy, Cambridge University Press, New York, 2014
- Péterfalvi Attila, Algoritmusok és adatvédelem: Quo vadis? 179-185. o. In: Török Bernát, Ződi Zsolt (szerk.), A mesterséges intelligencia szabályozási kihívásai, Ludovika Egyetemi Kiadó, Budapest, 2021
- Dr. Pázmándi Kinga, Modern reklámjog. A reklám a tisztességtelen verseny elleni jog és a modern reklámjog határán, HVG-ORAC Lap- és Könyvkiadó, Budapest, 2007

Az Innovációs és Technológiai Minisztérium ÚNKP-21-3 kódszámú Új Nemzeti Kiválóság Programjának a Nemzeti Kutatási, Fejlesztési és Innovációs Alapból finanszírozott szakmai támogatásával készült.

Felhasznált elektronikus források

- Augmented Reality (AR), Gartner Glossary, https://www.gartner.com/en/information-technology/glossary/augmented-reality-ar
- Cathy Hackl, Defining The Metaverse Today, 2021.05.02, https://www.forbes.com/sites/cathyhackl/2021/05/02/defining-the-metaverse-today/?sh=50bfe19c6448
- Dave Johnson, What is a deepfake? Everything you need to know about the AI-powered fake media, 2022.08.10, https://www.businessinsider.com/what-is-deepfake, 2022.08.16.
- DoNotPay, https://donotpay.com/
- Federal Trade Commission, Equifax to Pay $575 Million as Part of Settlement with FTC, CFPB, and States Related to 2017 Data Breach, https://www.ftc.gov/news-events/news/press-releases/2019/07/equifax-pay-575-million-part-settlement-ftc-cfpb-states-related-2017-data-breach, 2019.07.22
- Froggipedia, https://apps.apple.com/us/app/froggipedia/id1348306157
- Hilda Clune, Three use cases for virtual reality in enterprise, PwC Australia, Digital Pulse, 2017.05.26, https://www.pwc.com.au/digitalpulse/three-use-cases-virtual-reality-enterprise.html
- Jane Wakefield, MyHeritage offers 'creepy' deepfake tool to reanimate dead, 2021.02.26, https://www.bbc.com/news/technology-56210053, 2022.08.16.
- Joan Rogers, N.C. Law Regulates LegalZoom, Other Legal Doc Providers, Bloomberg Law, 2016.07.26, https://news.bloomberglaw.com/business-and-practice/n-c-law-regulates-legalzoom-other-legal-doc-providers
- Meta, https://store.facebook.com/quest/products/quest-2
- Nahia Orduña, Why Robots Won't Steal Your Job, 2021.03.19, https://hbr.org/2021/03/why-robots-wont-steal-your-job

Az Innovációs és Technológiai Minisztérium ÚNKP-21-3 kódszámú Új Nemzeti Kiválóság Programjának a Nemzeti Kutatási, Fejlesztési és Innovációs Alapból finanszírozott szakmai támogatásával készült.

- Nathaniel Kunes, How Is Smart Home Technology Shaping The Property Management Industry? Forbes, 2022.03.08, https://www.forbes.com/sites/forbesbusinesscouncil/2022/03/08/how-is-smart-home-technology-shaping-the-property-management-industry/?sh=1458eb0e382c
- New York State Office, Attorney General, 2018.09.26, A.G. Underwood Announces Record $148 Million Settlement With Uber Over 2016 Data Breach, https://ag.ny.gov/press-release/2018/ag-underwood-announces-record-148-million-settlement-uber-over-2016-data-breach
- Pokémon Go, https://pokemongolive.com/
- Rebecca Cairns, Meet Grace, the ultra-lifelike nurse robot, CNN, 2021.08.19, https://edition.cnn.com/2021/08/19/asia/grace-hanson-robotics-android-nurse-hnk-spc-intl/index.html
- Research leading blockchain use cases, IBM, https://www.ibm.com/blockchain/use-cases/
- Robots Help Nurses Get the Job Done–With Smiles and Beeps, Cedars Sinai, 2021.11.29, https://www.cedars-sinai.org/newsroom/robots-help-nurses-get-the-job-donewith-smiles-and-beeps/
- Taylor Key Lively, US State Privacy Legislation Tracker, 2022.08.11, https://iapp.org/resources/article/us-state-privacy-legislation-tracker/
- Thomas Brewster, How Equifax Kept Its Mega Breach Secret From Its Own Staff, Forbes, 2018.03.14, https://www.forbes.com/sites/thomasbrewster/2018/03/14/how-equifax-kept-its-mega-breach-secret-from-its-own-staff/?sh=271a34153ef1
- Virtual Reality (VR), Gartner Glossary, https://www.gartner.com/en/information-technology/glossary/vr-virtual-reality
- What is blockchain technology? IBM, https://www.ibm.com/topics/what-is-blockchain
- World Economic Forum, The Future of Jobs Report, 2020. október, https://www.weforum.org/reports/the-future-of-jobs-report-2020/digest
- WWF Free Rivers, https://apps.apple.com/us/app/wwf-free-rivers/id1349935575
- Yasmin Khorram, Kate Rooney, Young trader dies by suicide after thinking he racked up big losses on Robinhood, CNBC, 2020.06.18, https://www.cnbc.com/2020/06/18/young-trader-dies-by-suicide-after-thinking-he-racked-up-big-losses-on-robinhood.html

Az Innovációs és Technológiai Minisztérium ÚNKP-21-3 kódszámú Új Nemzeti Kiválóság Programjának a Nemzeti Kutatási, Fejlesztési és Innovációs Alapból finanszírozott szakmai támogatásával készült.

Felhasznált jogszabályok, bírósági és hatósági határozatok

Nemzetközi, valamint európai uniós jogforrások, bírósági és hatósági határozatok:

- International Civil Aviation Organization, Remotely Piloted Aircraft System (RPAS) Concept of Operations (CONOPS) for International IFR Operations, https://www.icao.int/safety/UA/Documents/ICAO%20RPAS%20CONOPS.pdf, 2022.08.20.
- OECD.AI. National AI policies & strategies, https://oecd.ai/en/dashboards, 2022.08.16
- 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 irányelv hatályon kívül helyezéséről (általános adatvédelmi rendelet), OJ L 119, 4.5.2016, p. 1–88 (BG, ES, CS, DA, DE, ET, EL, EN, FR, GA, HR, IT, LV, LT, HU, MT, NL, PL, PT, RO, SK, SL, FI, SV)
- 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, OJ L 119, 4.5.2016, p. 89–131 (BG, ES, CS, DA, DE, ET, EL, EN, FR, HR, IT, LV, LT, HU, MT, NL, PL, PT, RO, SK, SL, FI, SV)
- A Bizottság (EU) 2019/945 felhatalmazáson alapuló rendelete (2019. március 12.) a pilóta nélküli légijármű-rendszerekről és a pilóta nélküli légijármű-rendszerek harmadik országbeli üzembentartóiról, OJ L 152, 11.6.2019, p. 1–40 (BG, ES, CS, DA, DE, ET, EL, EN, FR, HR, IT, LV, LT, HU, MT, NL, PL, PT, RO, SK, SL, FI, SV)

Az Innovációs és Technológiai Minisztérium ÚNKP-21-3 kódszámú Új Nemzeti Kiválóság Programjának a Nemzeti Kutatási, Fejlesztési és Innovációs Alapból finanszírozott szakmai támogatásával készült.

- Javaslat az Európai Parlament és a Tanács rendelete a digitális szolgáltatások egységes piacáról (digitális szolgáltatásokról szóló jogszabály) és a 2000/31/EK irányelv módosításáról, Brüsszel, 2020.12.15., COM(2020) 825 final, 2020/0361(COD)
- Javaslat, az Európai Parlament és a Tanács Rendelete a mesterséges intelligenciára vonatkozó harmonizált szabályok (a mesterséges intelligenciáról szóló jogszabály) megállapításáról és egyes uniós jogalkotási aktusok módosításáról, Brüsszel, 2021.4.21. COM(2021) 206 final, 2021/0106(COD)
- Az Adatvédelmi Munkacsoport Iránymutatása az automatizált döntéshozatallal és a profilalkotással kapcsolatban a 2016/679 rendelet alkalmazásához, 17/HU.WP251rev.01
- Az Európai Adatvédelmi Testület 5/2020 Iránymutatása az (EU) 2016/679 rendelet szerinti hozzájárulásról
- Az Európai Adatvédelmi Testület és az Európai Adatvédelmi Biztos 5/2021. sz. közös véleménye a mesterséges intelligenciára vonatkozó harmonizált szabályok (a mesterséges intelligenciáról szóló jogszabály) megállapításáról szóló európai parlamenti és tanácsi rendeletre irányuló javaslatról
- Az Európai Adatvédelmi Testület 2022.05.12-én elfogadott, az arcfelismerő technológia bűnüldözési területen való alkalmazásáról szóló 2022/05. sz. iránymutatása

Magyar jogforrások, bírósági és hatósági határozatok:

- Magyarország Mesterséges Intelligencia Stratégiája, https://ai-hungary.com/api/v1/companies/15/files/137203/view
- A Nemzeti Adatvédelmi és Információszabadság ajánlása a drónokkal megvalósított adatkezelésekről, 2014
- NAIH/2015/2201/17/H ügyszámú határozat
- NAIH-85-3/2022 ügyszámú határozat

Az Innovációs és Technológiai Minisztérium ÚNKP-21-3 kódszámú Új Nemzeti Kiválóság Programjának a Nemzeti Kutatási, Fejlesztési és Innovációs Alapból finanszírozott szakmai támogatásával készült.

Egyéb tagállami bírósági és hatósági határozatok:

- A belga adatvédelmi hatóság (Autorité de protection des données) DOS-2019-01377 sz. ügyben hozott döntése, https://www.autoriteprotectiondonnees.be/publications/decision-quant-au-fond-n-21-2022-english.pdf
- A Norvég Adatvédelmi Hatóság Mesterséges Intelligencia és Adatvédelem című Jelentése (https://www.datatilsynet.no/globalassets/global/english/ai-and-privacy.pdf)
- CNIL, Blockchain and the GDPR: Solutions for a responsible use of the blockchain in the context of personal data, 2018.11.06, https://www.cnil.fr/en/blockchain-and-gdpr-solutions-responsible-use-blockchain-context-personal-data
- CNIL, Expérimentation de la reconnaissance faciale dans deux lycées : la CNIL précise sa position, 2019.10.29, https://www.cnil.fr/fr/experimentation-de-la-reconnaissance-faciale-dans-deux-lycees-la-cnil-precise-sa-position
- CNIL, SAN-2021-003 számú, 2021. január 21-én kelt határozata, https://www.legifrance.gouv.fr/cnil/id/CNILTEXT000042960768
- Tribunal Administratif de Marseille, N° 1901249, https://www.laquadrature.net/wp-content/uploads/sites/8/2020/02/1090394890_1901249.pdf

Amerikai jogszabályok, bírósági és hatósági határozatok:

- Algorithmic Accountability Act, https://www.congress.gov/bill/117th-congress/house-bill/6580/text
- Children's online Privacy Protection Rule (https://www.ecfr.gov/current/title-16/chapter-I/subchapter-C/part-312)
- National Artificial Intelligence Initiative Act, https://www.congress.gov/116/crpt/hrpt617/CRPT-116hrpt617.pdf#page=1210
- National Artificial Intelligence Initiative, https://www.ai.gov/

Az Innovációs és Technológiai Minisztérium ÚNKP-21-3 kódszámú Új Nemzeti Kiválóság Programjának a Nemzeti Kutatási, Fejlesztési és Innovációs Alapból finanszírozott szakmai támogatásával készült.

- California Consumer Privacy Act (https://leginfo.legislature.ca.gov/faces/codes_displayText.xhtml?division=3.&part=4.&lawCode=CIV&title=1.81.5)
- California Legislative Information, https://leginfo.legislature.ca.gov/faces/billNavClient.xhtml?bill_id=201920200AB730, 2022.08.19.
- California Privacy Rights and Enforcement Act of 2020 (https://iapp.org/resources/topics/ccpa-and-cpra/)
- Colorado Privacy Act (https://law.lis.virginia.gov/vacode/title59.1/chapter53/section59.1-576/)
- Virginia Consumer Data Protection Act (https://law.lis.virginia.gov/vacode/title59.1/chapter53/section59.1-576/)
- Copyright Review Board, United States Copyright Office, decision, correspondence ID 1-3ZPC6C3; SR # 1-7100387071, 2022.02.14, https://www.copyright.gov/rulings-filings/review-board/docs/a-recent-entrance-to-paradise.pdf
- NHTSA, Automated Vehicles for Safety, https://www.nhtsa.gov/technology-innovation/automated-vehicles-safety, 2022.08.18.
- Thaler v. Vidal, No. 21-2347 (Fed. Cir. 2022).

Az Innovációs és Technológiai Minisztérium ÚNKP-21-3 kódszámú Új Nemzeti Kiválóság Programjának a Nemzeti Kutatási, Fejlesztési és Innovációs Alapból finanszírozott szakmai támogatásával készült.