DOI: 10.38146/BSZ-AJIA.2025.v73.i5.pp977-999

A biometrikus azonosítás és az MI összefüggései, valamint kockázatértékelési lehetőségei

The connection of biometric identification and AI, and its risk assessment possibilities

Ujhegyi Péter
doktorandusz, műszaki vezető
Óbudai Egyetem,
Biztonságtudományi Doktori Iskola
ujhegyi.peter@uni-obuda.hu

Őszi Arnold
Dr., PhD, egyetemi adjunktus
Óbudai Egyetem,
Bánki Donát Gépész és Biztonságtechnikai Mérnöki Kar
oszi.arnold@bgk.uni-obuda.hu

Absztrakt

Cél: A tanulmány célja felhívni a figyelmet a biometrikus azonosítás és a mesterséges intelligencia (MI) fejlődésének összefüggéseire, valamint bemutatni a biometrikus azonosítási megoldások kockázatértékelésére kidolgozott módszereket.
Módszertan: Az elméleti módszerekről és összefüggésekről számos magyar és külföldi szakirodalmat, tudományos művet és jogszabályt dolgoztak fel a szerzők. Ennek során alkalmazták az analízis és szintézis módszereit, a tématerületeket alkotóelemeire bontották, és külön is mélységében tanulmányozták, így lehetővé vált a részek megismerése. Az elemzések során a különálló részeket és területeket újrarendezték és logikus egységbe foglalták. Ennek során megvizsgálták az összefüggéseket, és megállapították, hogy a biometria elterjedése elsősorban nem azonosítástechnológiai kérdés, hanem a biometrikus adatok feldolgozásának IT-módszertani kérdése, és az ezekhez kapcsolódó adatkezelési és adatbiztonsági kockázatok függvénye. Kutatómunkájukban fontos szerep jut az indukciónak, dedukciónak és az analógiának, mert kutatásuk során részeire bontották a problémákat, ezeket elemezték, és következtetéseket vontak le, mind mélyebben, ahogy az ismerttől haladtak az ismeretlen felé.
Megállapítások: Az MI szabályozás többszörösen összefügg a biometrikus azonosítással, a hazai és uniós jogalkotók törekednek a teljes értékláncon átívelő bizalmi ökoszisztéma szabályzói környezetének kialakítására, mely nagyfokú

A szerzők a kéziratot magyar nyelven nyújtották be. Benyújtás: 2024. 11. 15. Átdolgozás: 2024. 12. 10. Elfogadás: 2024. 12. 16.

bizalmat eredményezhet és csökkentheti a biometrikus azonosítási megoldások kockázatait.
Érték: A szerzők összefüggéseiben kutatták a biometrikus azonosítás, a személyes adatok kezelésének jogi hátterét és az MI-vel kapcsolatos összefüggéseket, s rámutattak a kockázatokkal való kapcsolatára. Kidolgoztak egy speciális keretrendszert a biometrikus azonosítási megoldások kockázatértékelésére.

A biometria témaköre nagyon szerteágazó, sok területen van már jelen. A hétköznapjainkban történő felhasználás egyre jobban terjed a beszivárgó kényelmi megoldások révén, az azonosítás és a hitelesítés terén egyaránt. A biometrikus azonosítás technikai megoldásaival szemben számtalan elvárás, ellenérzés és félelem alakult ki, melyek hatással vannak a megoldásokra és a megoldások elterjedésére, ugyanakkor az MI ilyen ütemű terjedésével még több biometrikus azonosítással összefüggő kockázat lép fel. Ahhoz, hogy jó és hasznos technológiai megoldásokat széles körben és biztonságosan, jogszerűen tudjunk használni, szükséges vizsgálni ezeket a tényezőket, az összefüggéseket és a kockázatokat. A cikkben a biometrikus azonosítás és az MI összefüggéseit vizsgálják a szerzők, és a kockázatértékelési lehetőségeket mutatják be.

Kulcsszavak: biometrikus azonosítás, adatvédelem, mesterséges intelligencia, szabályozás

Abstract

Aim: The aim of the study is to raise awareness of the links between the development of biometric identification and artificial intelligence (AI) and to present the methods developed for risk assessment of biometric identification solutions.
Methodology: The authors have reviewed a wide range of Hungarian and foreign literature, academic works and legislation on the theoretical methods and context. In doing so, the methods of analysis and synthesis were applied, the subject areas were broken down into their constituent parts and studied in depth separately, thus enabling the parts to be identified. In the course of the analyses, the separate parts and areas were reorganised and integrated into a logical whole. In doing so, the interlinkages were examined and it was concluded that the uptake of biometrics is not primarily an identification technology issue, but an IT methodological issue for processing biometric data and the associated data management and security risks. In their research, induction, deduction and analogy play an important role, as they have broken down the problems into parts, analysed them and drawn conclusions, going deeper and deeper as they move from the known to the unknown.

Findings: AI regulation is interlinked with biometric identification in multiple ways, and national and EU legislators are striving to create a regulatory environment of trust and confidence across the entire value chain, which can lead to a high level of trust and reduce the risks of biometric identification solutions.
Value: The authors have explored the context of biometric identification, the legal background to the processing of personal data and the relationship with AI, and have highlighted the risks associated with it. They developed a specific framework for risk assessment of biometric identification solutions.

The topic of biometrics is very diverse, it is already present in many areas. The use in our everyday lives is spreading more and more with infiltrating convenience solutions in the field of identification and authentication. Numerous expectations, objections and fears have arisen in relation to the technical solutions of biometric identification, which affect the solutions and the spread of the solutions, at the same time, with the spread of AI at this rate, even more risks related to biometric identification arise. In order to be able to use good and useful technological solutions widely and safely and legally, it is necessary to examine these factors, the connections and the risks. In our article, we examine the relationship between biometric identification and AI and present the risk assessment options.

Keywords: biometric identification, data protection, artificial intelligence, regulation

A biometrikus adatok védelmének és a mesterséges intelligencia fejlődésének összefüggései

Az uniós adatvédelmi szabályok alapesetben tiltják a biometrikus adatoknak a természetes személyek egyedi azonosítása céljából történő kezelését, és ez alól csak bizonyos feltételek mellett engednek kivételt. [Az általános adatvédelmi rendelet (EU) 2016/679 9. cikke, a bűnüldözésben érvényesítendő adatvédelemről szóló (EU) 2016/680 irányelv 10. cikke, illetve még az uniós intézményekre és szervekre alkalmazandó (EU) 2018/1725 rendelet 10. cikke alapján.]

Az általános adatvédelmi rendelet szerint ilyen adatkezelésre konkrétan csak korlátozott számú okból kerülhet sor, elsősorban alapvető közérdekből. Ezt a fajta adatkezelést uniós vagy nemzeti jog alapján lehet csak végezni, az arányosság követelményének és az adatvédelemhez való jog lényegének tiszteletben tartásával, megfelelő biztosítékok mellett. A bűnüldözésben érvényesítendő

adatvédelemről szóló irányelv értelmében ilyen adatkezelés csak szigorú szükségesség esetén, alapesetben uniós vagy nemzeti jog szerinti engedéllyel és megfelelő biztosítékok mellett végezhető. Mivel a biometrikus adatoknak valamely természetes személy egyedi azonosítása céljából történő bármely kezelése szabályozott esetet jelent az uniós jogban meghatározottak alapján, ezért az Európai Unió Alapjogi Chartájának hatálya alá tartozik. Következésképpen a jelenlegi uniós adatvédelmi szabályoknak és az Alapjogi Chartának megfelelően az MI csak akkor használható fel távoli biometrikus azonosítás céljára, ha az ilyen felhasználás kellően indokolt, arányos és megfelelő biztosítékok mellett történik. A távoli biometrikus azonosítást meg kell különböztetni a biometrikus azonosítástól, mert az MI-alkalmazások kifejezetten alkalmasak távoli biometrikus azonosításra és más intruzív megfigyelési célokra történő felhasználásra, ezért azt mindig „nagy kockázatúnak" kell minősíteni, vagyis ilyen esetekben mindig alkalmazandók a kötelező követelmények (URL1).

„*A mesterséges intelligencia fejlesztőire és alkalmazóira már ma is alkalmazandók az alapvető jogokra (pl. adatvédelem, magánélet védelme, megkülönböztetésmentesség), a fogyasztóvédelemre, valamint a termékbiztonságra és termékfelelősségre vonatkozó uniós jogszabályok. A fogyasztók ugyanilyen szintű biztonságot és jogokat várnak el, függetlenül attól, hogy egy termék vagy egy rendszer a mesterséges intelligenciára támaszkodik-e vagy sem. A mesterséges intelligencia bizonyos sajátosságai (pl. átláthatatlanság) azonban megnehezíthetik e jogszabályok alkalmazását és végrehajtását. Ezért meg kell vizsgálni, hogy a jelenlegi jogszabályok képesek-e kezelni a mesterséges intelligencia kockázatait, és a végrehajtásuk hatékonyan kikényszeríthető-e, vagy a jogszabályok kiigazítása, esetleg új szabályozás kialakítása szükséges.*

A mesterséges intelligencia által fokozottan lehetővé válik az emberek mindennapi szokásainak figyelemmel kísérése és elemzése. Fennáll például annak a kockázata, hogy a mesterséges intelligenciát uniós adatvédelmi és egyéb szabályokat megsértő módon, állami hatóságok vagy más szervek tömeges megfigyelésre, a munkáltatók pedig munkavállalóik viselkedésének megfigyelésére használhatják. Nagy adatmennyiségek elemzésével és az adatok közötti összefüggések azonosításával a mesterséges intelligencia személyek adatainak visszakeresésére és anonim jellegének megszüntetésére is felhasználható lehet, ami új személyesadatvédelmi kockázatokat teremt olyan adatkészletek esetében is, amelyek önmagukban véve nem tartalmaznak személyes adatokat." (URL2)

Véleményünk szerint itt kapcsolódik össze az MI felhasználása és a biometrikus azonosítás elterjedésének kérdése, mert az MI használatával és az adatelemzésekkel nagy mértékben nő a kockázat, hogy megfelelő szabályozás nélkül az anonim adatokból az algoritmusokkal biometrikus azonosítás történik.

Ez alapján alátámasztható, hogy a biometria elterjedésének tényezői jelentősen összefüggenek az adatvédelmi, adatkezelési és az MI szabályozásokkal, melyek kutatásaink alapján abba az irányba mutatnak, hogy ahogyan az informatikai biztonságot is kockázat alapon kell megítélni, úgy az MI keretrendszerét és a biometrikus megoldások szabályozását is kockázati alapon, a felhasználási terület függvényében kell kialakítani. Az viszont kimondható, hogy a 2021 előtti időszakra jellemző, adatvédelemre vonatkozó jogi, szabályzói hiányosságokat az EU hatékonyan elkezdte ledolgozni. Az Európai Bizottság 2021 áprilisában előterjesztett egy javaslatot az Európai Unió MI szabályozási keretrendszeréről. Az MI-tervezet az első olyan kísérlet, amely egy átfogó szabályozást hozna létre a területen. A javasolt jogi keret az MI-rendszerek konkrét felhasználására és az ezzel járó kockázatokra összpontosít. Az Európai Bizottság azt javasolja, hogy az EU a jogszabályokban technológiától függetlenül definiálja az MI-rendszereket, és osztályozást állítson fel különböző követelményekkel és kötelezettségekkel egy „kockázatalapú megközelítésen" alapulva. Néhány MI-rendszer, amely „elfogadhatatlan" kockázatokat mutatna, tilos lenne. Számos „magas kockázatú" MI-rendszer engedélyezett lenne, de bizonyos követelmények és kötelezettségek mellett, hogy hozzáférést szerezzen az EU piacához. Azok az MI-rendszerek, amelyek csak „korlátozott kockázatot" jelentenek, nagyon könnyű átláthatósági kötelezettségeknek lennének kitéve. Az Európa Tanács 2021 decemberében elfogadta az EU-tagállamok általános álláspontját, majd az Európai Parlament 2023 júniusában szavazott róla. Az EU jogalkotók most tárgyalásokat kezdenek az új jogszabály véglegesítéséhez, jelentős módosításokkal az Európai Bizottság javaslatához képest, beleértve az MI-rendszerek definíciójának felülvizsgálatát, a tiltott MI-rendszerek listájának kibővítését, valamint kötelezettségeket az általános célú MI és generatív MI modellekre.

Az EU szabályozási folyamata rámutatott arra, hogy az MI meghatározása mellett fontos a „kockázat", a „magas kockázat", az „alacsony kockázat", a „távoli biometrikus azonosítás" és a „kár" fogalmának meghatározása is. A szakértői csoportok és a konzultációban részt vevő piaci szereplők többsége kifejezetten támogatta a kockázatalapú megközelítést. A válaszadók úgy vélték, hogy a kockázatalapú keretrendszer alkalmazása jobb megoldást nyújt, mint az általános szabályozás, amely minden MI-rendszert érint. A kockázatokat és fenyegetéseket ágazati és eseti alapú megközelítéssel kell kezelni. A kockázatok kiszámításánál figyelembe kell venni a jogokra és a biztonságra gyakorolt hatást.

Kutatásaink alapján ez kifejezetten igaz általánosságban a biometrikus rendszerekkel kapcsolatos kockázatokra is.

A nagy kockázatú MI-rendszerek és a távoli biometrikus azonosítás kockázatai az MI-re vonatkozó harmonizált szabályok megállapításai közül [2021/0106

(COD)]: A távoli biometrikus azonosító rendszer e rendeletben használt fogalmát funkcionális értelemben kell meghatározni, olyan MI-rendszerként, amelynek célja természetes személyek távolról történő azonosítása a személy biometrikus adatainak egy referencia-adatbázisban szereplő biometrikus adatokkal való összevetése révén, annak előzetes ismerete nélkül, hogy a célszemély jelen lesz-e és azonosítható-e, függetlenül az alkalmazott konkrét technológiától, folyamatoktól vagy a biometrikus adatok típusától. Figyelembe véve eltérő jellemzőiket és használati módjaikat, valamint a különböző kockázatokat, különbséget kell tenni a „valós idejű" és a „nem valós idejű" távoli biometrikus azonosító rendszerek között. A „valós idejű" rendszerek esetében a biometrikus adatok rögzítése, összehasonlítása és azonosítása azonnal, majdnem azonnal vagy mindenesetre jelentős késleltetés nélkül történik. E tekintetben nem engedhető meg, hogy a szóban forgó MI-rendszerek „valós idejű" használatára vonatkozó kisebb késleltetésekre legyen lehetőség, és ezáltal az e rendeletben foglalt szabályokat bárki megkerülje. A „valós idejű" rendszerek olyan „élő" vagy megközelítőleg „élő" anyagot, például videofelvételt használnak, amelyet kamera vagy hasonló funkciójú más eszköz generál. A „nem valós idejű" rendszerek esetében ezzel szemben a biometrikus adatokat már rögzítették, és az összevetésre és az azonosításra csak jelentős késleltetéssel kerül sor. Olyan anyagokról van szó, mint például a zárt láncú televíziós kamerák vagy magánkészülékek által előállított képek vagy videofelvételek, amelyek a rendszernek az érintett természetes személyek tekintetében történő használata előtt keletkeztek.

Az MI-rendszereknek természetes személyek „valós idejű" távoli biometrikus azonosítására, a nyilvánosság számára hozzáférhető helyeken, bűnüldözés céljából történő használata különösen betolakodik az érintett személyek jogaiba és szabadságába, mivel hatással lehet a lakosság nagy részének magánéletére, az állandó megfigyelés érzetét keltheti, és közvetve visszatarthat a gyülekezési jog szabadsága és más alapvető jogok gyakorlásától. Ezenkívül a hatás azonnali jellege és az ilyen „valós időben" működő rendszerek használatával kapcsolatos további ellenőrzések vagy korrekciók korlátozott lehetőségei fokozott kockázatot jelentenek a bűnüldözési tevékenységek által érintett személyek jogaira és szabadságára nézve. E rendszerek bűnüldözési célú használatát ezért meg kell tiltani, kivéve három, kimerítő jelleggel felsorolt és szűken meghatározott helyzetet (áldozatok felkutatása, terrortámadás veszélye, illetve speciális esetekben bűncselekmények felderítése), amelyekben a használat feltétlenül szükséges egy olyan jelentős közérdek érvényesítéséhez, amelynek fontossága meghaladja a kockázatokat (URL3).

Az MI-alapú rendszerek, melyeket elemzésekre, következtetésekre és másodlagos, harmadlagos folyamatok során azonosítási feladatokra lehet alkalmazni,

vagy a bűnüldözésben megelőzés céllal használni, véleményünk szerint különösen sok társadalmi vitát és megosztottságot fog okozni. Nagyon érzékenyen kell ezt a területet kezelni, és minél előbb az összes érintett bevonásával, széles körben társadalmi és szakmai fórumokon keresztül egyeztetéseket folytatni a szabályozásról, mert a nem jól kezelt és alulszabályozott folyamatok, a megoldások visszaéléssel kapcsolatos lehetőségei miatt hatványozottan negatívan hathatnak a biometria elterjedésére.

A kockázatértékelés keretrendszere

Olyan világot élünk, ahol fokozódnak a nemzetközi konfliktusok, egyre több fronton nyílnak fegyveres összetűzések, az országok és a régiók bővítik a hadi kiadásokra fordított kereteket, ezért a lakosság biztonságérzete csökken. Ilyen helyzetben természetes lehet a biztonságnövelő megoldások növekvő elfogadottsága (biztonság utáni vágy mint alapszükséglet), éppen ezért ezek kockázataival is érdemes tisztában lenni. A kockázatok értékelésére szabványok, keretrendszerek állnak rendelkezésre. Munkánk során az International Standard, IEC/FDIS 31010:2009 szabványt vettük alapul (URL9).

A kockázatbecslés a kockázatazonosításból, a kockázatelemzésből és a kockázatértékelésből áll. A kockázatok általában szervezeti szinten, osztályok szintjén, projekteknél, vagy egyedi tevékenységeknél értékelhetők. Különböző eszközök és technikák alkalmazhatók a különböző kontextusokban.

A kockázatazonosítás magában foglalja a kockázat okainak és forrásainak felkutatását és leírását. Ennek módszerei: az evidenciaalapú módszer, ahol checklisták és történelmi adatok alapján történik az áttekintés; a rendszeres csoportmódszer, ahol egy szakértőkből álló csapat rendszeres folyamatkövetést végez a kockázatok azonosításához egy strukturált kérdéssorozat alkalmazásával; és végül az induktív következtetési technikák módszer, mint például a Hazard and Operability (HAZOP) módszer.

A kockázatelemzés tartalmazza a kockázati események következményeinek és valószínűségeinek a meghatározását és kombinálását annak megállapítására, hogy milyen szintű a kockázat. A kockázatok elemzésére alkalmazott módszerek lehetnek minőségi, félkvantitatív vagy kvantitatív jellegűek. A részletesség mértéke a konkrét alkalmazástól, a rendelkezésre álló megbízható adatoktól és még szervezeti, vagy a felhasználási területi tényezőktől is függ. A minőségi értékelés a következményt, a valószínűséget és a kockázat szintjét olyan jelentőségi szintekkel határozza meg, mint „magas”, „közepes” és „alacsony”, összevonhatja a következményeket és a valószínűséget, és a kapott kockázatszintet

minőségi kritériumokkal veti össze. Mi is ezt a módszert használtuk, így a kockázatértékelés magában foglalja a becsült kockázati szintek összehasonlítását a meghatározott kockázati kritériumokkal, annak érdekében, hogy meghatározzuk a kockázat mértékének és típusának jelentőségét.

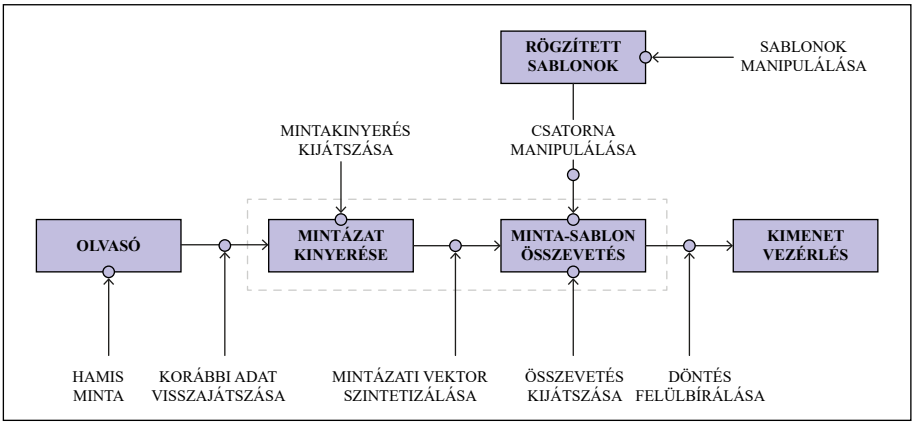
1. számú táblázat
A szempontrendszer alapjai

Valamennyi szemponthoz három értékelési kimenet (válasz) rendelhető	
Kockázat szempontból nem elfogadható	**magas**
Kockázat szempontból nem optimális	**közepes**
Kockázat szempontból optimális	**alacsony**

Forrás. A szerzők saját szerkesztése.

Az általunk kidolgozott szempontrendszer azt mutatja be, hogy a különböző felhasználási területeken alkalmazott biometrikus azonosítási megoldások különböző szempontok alapján milyen eltérő kockázatot képviselnek. A biometrikus azonosítási rendszerek sérülékenységi lehetőségeit figyelembe véve, a kockázatok vizsgálata szempontjából kizárjuk azokat a tényezőket, melyek az azonosítási rendszer informatikai komponenseivel (1. számú ábra) vannak összefüggésben, illetve a felhasználási területtel összefüggő szempontokat is, és csak az azonosításokat, az azonosítási eljárás fajtája és a mintaadás szempontjából vizsgáljuk.

1. számú ábra
Egy általános biometrikus azonosítási rendszer sérülékenységi lehetőségei



Forrás. Ratha et al., 2001.

A biometrikus azonosítási megoldások és a kockázatok kapcsolata

A felhasználók szempontjából a biometrikus azonosítási megoldások jellemzői alapján vizsgálható a kockázat. Fontos kiemelni, hogy általában a kockázatelemzés nagyban függ a helyi specifikumoktól, mint a felhasználás környezete, a felhasználás célja és módja, függ a kiszolgáló informatikai környezet paramétereitől és még számos tényezőtől is. Az általunk meghatározott 14 paraméterrel – megítélésünk szerint – elvégezhető egy független, általános vizsgálat a biometrikus azonosítási megoldások kockázataival kapcsolatban. Meglátásunk szerint ezek a kockázatok összefüggésben vannak az azonosítási megoldások elterjedésével.

Egyetemesség (universality)

A vizsgált környezetben a biometrikus minta minden alany esetében kinyerhető legyen. Az egyetemesség mérésére alkalmazható mérőszám a Failure to Enroll (FTE), amely megmutatja az adott környezetre vonatkoztatva, hogy milyen arányban fordulnak elő azon személyek, akik mintái az adott biometrikus azonosítási technikával nem ismerhetőek fel, így már a sablon kinyerése is akadályba ütközik. Az általános cél az, hogy a felhasználási terület ismeretében minél szélesebb körben, minden felhasználóra alkalmazható legyen az azonosítási technika, de kockázat szempontjából minél több személy esetén alkalmazható, annál nagyobb kockázatot jelent (Jain et al., 2011).

Az azonosításhoz használt minták az emberi test geometriai vagy viselkedési jellemzőiből, vagy ezekből származtatott, következtetett adatokból származnak, de a népességet tekintve ez nem minden esetben áll rendelkezésre. Az arcfelismerésnél, az érhálózat-alapú megoldásoknál, a DNS-azonosításnál, a hangalapú megoldásoknál és a szokáselemzésen alapuló megoldásoknál egyetemesség szempontjából kevesebb kizáró tényező áll rendelkezésre a többi megoldáshoz képest. Aláírás esetén az írástudatlanság, kézgeometria, retina, írisz és ujjnyomat esetén testi, biológiai eredetű hiányosságok és fogyatékosságok miatt vannak kizáró tényezők, például a népesség 1–3 százalékának nem áll rendelkezésre és nem megfelelő az ujjnyomata (Zhang & Lu, 2013).

Egyediség (uniqueness)

A biometrikus minta egyedisége biztosítja az egyének megkülönböztetését. Minden mintának szükséges, hogy legyen egyedi azonosításra alkalmas mintázata, amely alapján megkülönböztethető más mintáktól. A minták hasonlósága magas

FAR (téves elfogadási arány – False Acceptance Rate) és FRR (téves elutasítási arány – False Rejection Rate) értékeket eredményez, amely kihat az azonosítás biztonságára és egyben a kockázataira is (Zhang & Lu, 2013). A leginkább egyedi mintázatok – az írisz, az ujjnyomat, az arc, az érhálózat – egyediség szempontjából a kisebb kockázatot jelentik (URL4; Crisan, 2016; Karimi ez al., 2022). Kevés kutatás áll még rendelkezésre, véleményünk szerint a kevésbé egyedi minták alapján történő azonosítási megoldások nagyobb kockázatot képviselnek (Harakannanavar et al., 2019).

Elfogadottság (acceptability)

Az azonosítási megoldásokkal kapcsolatban számos félelem és ellenérzés alakulhat ki egyéni és társadalmi szinten is. Az elfogadottság azt jelenti, hogy a rendszert használó egyén mennyire együttműködő az azonosítási folyamat során, vagy az ellenérzései miatt befolyásoló tényező lép fel a mintaadás elvégzése során. Fontos szempont, hogy az azonosítás során az egyén bevonódása a folyamatba ne legyen túlzott mértékű. A retina azonosítással kapcsolatban ismertek a félelmek, sokan vélik ártalmasnak a szem megvilágítását (vagy legalább tartanak egészségkárosító hatásától), és a szenzor szemhez túl közeli pozicionálása sem közkedvelt. Az ujjnyomat- és DNS-alapú azonosítási technológiák alkalmazása szorosan kapcsolódik a bűnüldözési és kriminalisztikai tevékenységekhez, amelyek jelentős mértékben befolyásolják a módszer percepcióját és elfogadottságát a társadalomban (Jain et al., 2011; Zhang & Lu, 2013).

Kijátszhatóság (circumvention)

A biometrikus azonosítási megoldások kapcsán a kijátszhatóság (spoofing vagy impersonation attack) egy olyan biztonsági kihívást jelent, amelyben egy támadó szándékosan próbálja megtéveszteni a biometrikus rendszert, hogy az tévesen hitelesítse őt egy másik, jogos felhasználóként. Ez általában úgy történik, hogy a támadó utánozza vagy reprodukálja a jogos felhasználó biometrikus adatait – például ujjlenyomatot, arcképet, íriszképet vagy hangmintát –, és ezeket az adatokat használja fel az azonosító rendszer megtévesztésére. A kijátszhatóság mértékét a rendszer hamisítási kísérletekkel szemben tanúsított ellenálló képessége határozza meg. A magas szintű biztonságú biometrikus rendszerek fejlett detektálási mechanizmusokkal rendelkeznek a hamisítási kísérletek felismerésére, így csökkentve a sikeres támadások valószínűségét (Őszi, 2019; Peña et al., 2021; Markowitz, 2000; Yan et al., 2019; URL5).

Elérhetőség (availability)

Az ismert technológiák segítségével hatékonyan megszerezhető az az információ, amely a biometrikus minták egyediségét kódolja, ami kulcsfontosságú szerepet játszik abban, hogy mennyire egyszerű a mintából az azonosításhoz szükséges képet előállítani. Fontos megjegyezni, hogy nem minden biometrikus jellemző áll rendelkezésre egyszerűen. Könnyen kinyerhető adatok esetén az illetékteleneknek is könnyebb lesz hozzáférniük és felhasználniuk őket, így nagyobb a kockázat, míg nehezen kinyerhető adatoknál az illetéktelenek számára is nehezebb lesz hozzáférni és felhasználni azokat. Arcfelismerés esetén a minta elérhetősége jobb, egy fénykép vagy videó alapján is könnyen elvégezhető, míg mondjuk retina azonosítás esetén a fej pontos pozicionálása és a szem megvilágítása szükséges (Zhang & Lu, 2013).

Élőminta felismerés (live pattern recognition)

A biometrikus azonosítások kapcsán az „élőminta felismerés" paramétere egy biztonsági mechanizmus, amely annak értékelésére szolgál, hogy a biometrikus rendszerbe bevitt minta valós, élő személytől származik-e, és nem egy hamisított vagy mesterségesen létrehozott reprodukciót használtak-e az azonosítási kísérlet során. Ez a paraméter segít megelőzni a csalási kísérleteket, mint például a biometrikus spoofingot vagy maszkhasználatot, ahol az azonosító rendszer megtévesztésére törekvő személyek hamis vagy manipulált biometrikus mintákat használnak a jogosulatlan hozzáférés megkísérlésére. A retinaalapú azonosításnál az élőminta felismerés magában foglalhatja a retinán belüli véráramlás vizsgálatát, vagy más élettani reakciók észlelését, az íriszalapú azonosítás esetében a pupillareflex vizsgálatát, az írisz mintázat spontán változásainak észlelését, vagy a szemhéj villódzásának és mozgásának analízisét. A hangalapú biometrikus azonosítás során az élőminta felismerés azt a képességet jelenti, hogy a rendszer képes megkülönböztetni a valódi, élő emberi hangot a felvételektől vagy szintetizált hangoktól. Ez magában foglalhatja a háttérzaj elemzését, a beszéd mintázatának, a hangszín változásainak, vagy akár a légzés és egyéb jellegzetes hangjellemzők figyelembevételét, amelyek nehezen reprodukálhatók vagy szimulálhatók Az élőminta felismerés technológiák különböző módszereket alkalmazhatnak még, mint például a mozgás analízisét, a bőrhőmérséklet vizsgálatát, a pulzus érzékelését, vér áramlását, pislogást vagy más élettani és viselkedési jellemzők detektálását, hogy biztosítsák a minta élő eredetét (Őszi & Kovács, 2011). Amennyiben az azonosítás megvalósítható élőminta felismerés nélkül és könnyen elérhető a technológia, akkor magas a kockázat.

Érintésnélküli technológia (contactless)

A biometrikus azonosítási technikák érintésmentes megoldása olyan módszer, amely lehetővé teszi egyén azonosítását vagy hitelesítését fizikai érintkezés nélkül, azaz a felhasználónak nem szükséges közvetlenül érintkeznie egy olvasó eszközzel vagy szenzorral. Kényelem és az azonosítás sebessége szempontjából előnyös lehet a megoldás. Az eszközök fizikai érintése szempontjából több dimenzióban vizsgálható a kockázat, mert a készülékek érintése nélkül csökken a keresztfertőzés kockázata, ami különösen fontos a COVID utáni időszakban is, hiszen az ilyen megoldások higiénikusabbá teszik a használatot. Mivel nincs szükség fizikai érintkezésre, csökkenhet az eszköz fizikai sérülésének vagy a manipulációnak a lehetősége és így azok kockázata is. Az érintésmentes technológiák esetében a támadók kísérletet tehetnek arra, hogy hamis biometrikus mintákkal (például fotók, videók vagy hangfelvételek használata) megtévesszék a rendszert. Az érintésmentes rendszerek nem minden esetben képesek olyan könnyen ellenőrizni a minta „élő" voltát, mint az érintésalapú rendszerek. Az érintésmentes technológiák érzékenyebbek lehetnek a környezeti tényezőkre, mint a fényviszonyok vagy háttérzaj. A támadók kihasználhatják ezeket a sebezhetőségeket, például manipulálva a környezeti feltételeket annak érdekében, hogy javítsák a hamis biometrikus adatok felismerésének esélyét.

Alany beleegyezésével megszerezhető minta (sample obtainable with consent)

A megszerezhető minták gyűjtése és felhasználása az érintett személy előzetes, tájékoztatáson alapuló, önkéntes és konkrét beleegyezésével történik. Ez a folyamat magában foglalja az alany tájékoztatását a biometrikus adatok gyűjtésének céljáról, módszereiről, a tárolás időtartamáról, valamint az adatokhoz való hozzáférésről és azok védelméről. Az alany beleegyezése azt jelenti, hogy aktív és egyértelmű hozzájárulást ad az adatainak gyűjtéséhez és felhasználásához, amely hozzájárulás bármikor visszavonható. Az azonosítás folyamata minél inkább megvalósítható beleegyezés nélkül, annál nagyobb kockázatot jelent.

Jelenlétalapú azonosítás (presence/non presence based)

A jelenlétalapú (Presence-Based) azonosítások olyan biometrikus azonosítási módszerek, amelyek az érintett személy fizikai jelenlétét igénylik a biometrikus adatok gyűjtéséhez és az azonosításhoz. Ezek a módszerek gyakran magasabb szintű biztonságot és kevésbé manipulálhatóságot biztosítanak, mivel a biometrikus mintavétel közvetlen interakciót igényel az azonosító rendszerrel. A jelenlét

nélküli (Non-Presence-Based) azonosítási módszerek pedig azok, amelyek nem igénylik az érintett személy fizikai jelenlétét a biometrikus adatok gyűjtése és azonosítása során. Ezen módszerek esetében az azonosítás történhet távoli vagy előre rögzített biometrikus adatok (például videók, fényképek) alapján. Ez a megközelítés rugalmasabb és kényelmesebb lehet a felhasználók számára, de bizonyos esetekben növelheti a csalás és az adatmanipuláció kockázatát.

Alkalmasság távoli, rejtett azonosításra (remote, covert identification)

A távoli, rejtett azonosítás lehetővé teszi az egyének azonosítását vagy ellenőrzését távolról, vagy anélkül, hogy tudomást szereznének az azonosítási folyamatról. A rejtett azonosítás (Covert Identification) során az egyéneket anélkül lehet azonosítani, hogy ők maguk tudnának az azonosítási folyamat létezéséről. Ez a módszer gyakran biztonsági, megfigyelési vagy bűnüldözési célokból kerül alkalmazásra, ahol fontos, hogy az azonosítás észrevétlen maradjon az érintett személy számára. A felhasználók szempontjából a távoli, rejtett azonosításra alkalmas megoldások jelentik a nagyobb kockázatot.

Minta változatlansága/állandósága az időben (permanence)

A paraméter azt jelenti, hogy a biometrikus adatok kinyerése mennyire marad konzisztens az idő múlásával, azaz a biometrikus minták milyen mértékben képesek fenntartani azonosítási pontosságukat hosszú időn keresztül, figyelembe véve az egyén fizikai és biológiai változásait, mint például az öregedés, sérülések, vagy egyészségügyi, életmódbeli változások hatásait. A szempont ott fontos a hosszú távú biometrikus alkalmazások felhasználásának tervezésekor, ahol az egyének éveken vagy évtizedeken keresztül kerülnek azonosításra ugyanazon biometrikus adatok alapján. A letárolt minta rendszeres aktualizálásával javítható a minta állandósága egy adott rendszerben, ha erre a felhasználási terület lehetőséget biztosít. Amennyiben erre nincs lehetőség, a minta állandóságával egyenes arányban nő a kockázat (Jain et al., 2011; Zhang & Lu, 2013).

Külső vagy belső biometrikus jellemző (external or internal biometric)

A külső biometrikus azonosítás a test külső jellemzőire támaszkodik, míg a belső biometrikus azonosítás a test belső tulajdonságait használja fel. A külső jegyek könnyebben mérhetők és megfigyelhetők, de az idővel könnyebben változhatnak. A belső biometrikus jegyek általában stabilabbak és egyediek, nehezebben változtathatók meg. A külső jegyek gyakran nyilvánosan hozzáférhetők, emiatt

lehet magas az adatvédelmi kockázatuk, az egyének akár a tudtuk nélkül is azonosíthatók. A belső adatok kezelése és tárolása mégis magasabb szintű adatvédelmi kockázatot jelent, mivel ezek az adatok érzékeny biológiai és egészségügyi információkat is tartalmazhatnak. A kockázatok mértékének értékelésekor fontos figyelembe venni, hogy a belső jegyeken alapuló biometrikus azonosítás technikailag megbízhatóbb és nehezebben hamisítható, de az adatvédelmi és etikai kockázatok miatt általában nagyobb aggodalomra ad okot. A belső adatok kompromittálása esetén az egyének személyes autonómiája és biztonsága súlyosabban érintett lehet, mint a külső adatok esetében. Ezért, bár a belső jegyeken alapuló azonosítás biztonsági szempontból előnyösebbnek tűnhet, a vele járó adatvédelmi és etikai kockázatok miatt összességében nagyobb a kockázat és emiatt nagyobb körültekintést igényel.

Használható biometrikus kategorizálásra (used for biometric categorization)

A kategorizálás csak a puha vagy gyenge biometrikus adatoknál alkalmazható, és használata olyan adatoknál lehetséges, amelyek önmagukban nem alkalmasak az egyértelmű azonosításra, de alkalmasak kategóriába sorolása, mint például életkor vagy az etnikai származás. Amennyiben az azonosítási megoldás alkalmas kategorizálásra, akkor az nagyobb kockázatot jelent (Wendehorst & Duller, 2021).

Használható biometrikus-alapú érzelemfelismerésre és következtetésre (used for biometric based emotion recognition and inference)

A biometrikus azonosítás során a rendszer az adott emberi egyedre jellemző feltételeket méri, vagy következtet az adatokból, beleértve a genetikai, fizikai, fiziológiai, viselkedési, pszichológiai vagy érzelmi jellegű tulajdonságokat és az ezekből kapott elemzett vagy következtetett adatokat is. Ezekből az adatokból többek között vallási, politikai, vagy akár szexualitással összefüggő információk származtathatók, melyek érzékeny adatoknak tekinthetők, és az ilyen rendszerek használata nagyobb kockázatot jelenthet (Wendehorst & Duller, 2021).

A fenti kockázati paraméterekhez tartozó meghatározás a 2. számú táblázatban látható.

2. számú táblázat

Biometrikus azonosítási megoldások 14 szempontjának kockázati paraméter meghatározása

Paraméterek	Kockázati szint	Meghatározás
Elfogadottság	Magas	Vannak ismert elutasítottsággal kapcsolatos tényezők, vagy a megoldás invazívabb jellegű
	Közepes	Kevésbé elutasított vagy invazívabb a mintaadás folyamata
	Alacsony	Nem elutasított, nem különösebben invazív vagy nem áll rendelkezésre információ a mintaadás folyamatával kapcsolatban
Kijátszhatóság	Magas	Mintaadás szempontjából sok ismert, vagy könnyű kijátszási módszer létezik
	Közepes	Mintaadás szempontjából kevés kijátszási módszer áll rendelkezésre, vagy csak nehezen megvalósítható
	Alacsony	Nem áll rendelkezésre módszer, vagy nem ismert
Elérhetőség	Magas	Ismert technológiák segítségével hatékonyan és könnyen szerezhető meg az információ
	Közepes	Kevesek által elérhető bonyolult módszerekkel, de könnyen szerezhető meg az információ
	Alacsony	Kevesek által elérhető bonyolult módszerekkel és nehezen szerezhető meg az információ
Élőminta felismerés	Magas	Könnyen elérhető technológiával megvalósítható az azonosítás élőminta felismerés nélkül
	Közepes	Kevesek számára elérhető technológiával valósítható meg az azonosítás élőminta felismerés nélkül
	Alacsony	Nem valósítható meg az azonosítás élőminta felismerés nélkül, vagy nincs információ róla
Érintésmentes	Magas	Könnyen elérhető technológiával megvalósítható az azonosítás érintésmentesen
	Közepes	Kevesek számára elérhető technológiával valósítható meg az azonosítás érintésmentesen
	Alacsony	Nem valósítható meg az azonosítás érintésmentesen
Beleegyezés	Magas	A minta begyűjthető az egyén tudta nélkül
	Közepes	Nem értelmezhető ennél a szempontnál
	Alacsony	A minta kifejezetten az egyén aktív közreműködésével gyűjthető be
Jelenlét	Magas	Az azonosításhoz nem szükséges a személy fizikai jelenléte
	Közepes	Nem értelmezhető ennél a szempontnál
	Alacsony	Az azonosításhoz szükséges a személy fizikai jelenléte
Távoli, rejtett	Magas	Az azonosítás elvégezhető távolról az egyén tudta nélkül
	Közepes	Nem értelmezhető ennél a szempontnál
	Alacsony	Az azonosítás nem végezhető el távolról az egyén tudta nélkül
Állandóság	Magas	A minta az idő múlásával nem, vagy csak nagyon kis mértékben, hosszú idő alatt változik. Nincs jelentős ismert külső behatás
	Közepes	A minta az idő múlásával változik, vagy van a mintára hatást gyakorló tényező
	Alacsony	A minta könnyen változik az idő múlásával, vagy több külső tényező könnyen hatást gyakorol
Külső/belső	Magas	Belső biometrikus adatok alapján történő azonosítás magasabb kockázatot jelentenek
	Közepes	Nem értelmezhető ennél a szempontnál
	Alacsony	Külső biometrikus adatok alapján történő azonosítás alacsonyabb kockázatot jelentenek
Kategorizálás	Magas	Az azonosítási megoldás használható kategorizálásra
	Közepes	Nem értelmezhető ennél a szempontnál
	Alacsony	Az azonosítási megoldás nem használható kategorizálásra, vagy nem ismert ilyen megoldás
Következtetés	Magas	Az azonosítási megoldás következtetésre kategorizálásra
	Közepes	Nem értelmezhető ennél a szempontnál
	Alacsony	Az azonosítási megoldás nem használható következtetésre, vagy nem ismert ilyen megoldás

Forrás. A táblázat a szerzők saját szerkesztése.

A biometrikus rendszerek fejlődésével, az eszközök tesztelési eredményeinek kiértékelésével és a gyakorlati tapasztalatok bővülésével szükségesnek tartjuk ezen szempontok pontosítását és kiegészítését, illetve figyelembevételét a biometrikus azonosítási eljárások felhasználási módjának. Álláspontunk szerint nem lehet időtálló érvényességű kockázatelemzést végezni, csak abban az esetben, ha módszer és eszközspecifikus alkalmazhatósági szempontrendszert állítunk fel (Balla, 2019).

A 3. számú táblázatban a biometrikus azonosítási technikák 14 szempont (Harakannanavar et al., 2019; Ahmad et al., 2018) alapján elvégzett minőségi értékelés jellegű kockázatelemzése látható.

3. számú táblázat

Biometrikus azonosítási megoldások kockázatelemzése

		Biológiai-fizikai jellemző alapú biometrikus adatok								Viselkedési jellemző alapú biometrikus adatok				
		Ujjnyomat	Érhálózat - tenyérvéna, ujjvéna	Arcfelismerés	Írisz	Retina	Kézgeometria elemzés	Szívritmus, egészségügyi adatok	DNS	Hang, beszédhang	Mozgás-, járás-, sziluett elemzés	Aláírás	Írásképi újramintavételezés/gépelés	Szokások elemzése
Általános paraméterek szerinti kockázatok	Egyetemesség (universality), mindenkinél alkalmazható legyen													
	Minta egyedisége (uniqueness)													
	Elfogadottság (acceptability)													
	Kijátszhatóság (circumvention)													
Begyűjtés módja szerint a kockázatok	Elérhetőség (availability)													
	Élőminta felismerés (live pattern recogn.)													
	Érintés nélküli technológia (contactless)													
	Alany beleegyezésével gyűjthető (sample obtainable with consent)													
	Jelenlétalapú azonosítás (presence/non presence based)													
	Alkalmas távoli, rejtett azonosításra (convert identification)													
Mérta lecsökkenthetőség szemp. a kockázatok	Minta változatlansága / állandósága az időben (permanence)													
	Külső vagy belső biometrikus jellemző													
Biometrikus adat felhasználásának módja szerinti kockázatok	Használható biometrikus kategorizálásra	N/A	N/A		N/A	N/A	N/A	N/A	N/A		N/A	N/A		
	Használható biometrikus-alapú érzelem felismerésre és következtetésre (vallás, politika szexualitás)	N/A	N/A		N/A	N/A	N/A		N/A			N/A		

*N/A: nem ismert

Forrás. A táblázat a szerzők saját szerkesztése (Tripathi, 2011; Srivastava, 2013).

Az elemzési módszertan kutatásaink alapján megfelelő a kockázatok egyszerű rangsorolására, mert ez a fajta elemzés széles körben használható egyszerű módszertanként annak meghatározására, hogy az adott kockázat elfogadható-e vagy sem olyan esetekben, amikor nem áll rendelkezésre minden információ (URL10).

A szempontrendszer alapján a legkevésbé kockázatos megoldás a kézgeometria, azután a retina- és az érhálózat-alapú biometrikus azonosítási megoldás. A leginkább kockázatos megoldás a hangalapú, az arcfelismerésen és a szokások elemzésén alapuló megoldások. Annak érdekében, hogy a kockázatokat megfelelő módon kezelni lehessen az MI szabályozásnak a biometrikus azonosítással mutatott összefüggései miatt, az Európai Parlament MI-re kialakított javaslatát véleményünk szerint alkalmazni lehet a biometriai azonosítási megoldásokra, de már a felhasználási terület figyelembevételével. A felhasználási lehetőségek kockázatalapú szempontjainak figyelembevételével a következő csoportosítás végezhető el (URL6).

Elfogadhatatlan kockázat – Tiltott biometrikus megoldások

Biometrikus azonosítási rendszerek, melyek alkalmazása összefügghet az emberek biztonságával, megélhetésével és jogaival, és egyértelmű fenyegetésnek tekinthetők ezekre.

- Káros manipulatív technikákkal összefüggésben alkalmazható megoldások (reklámozásban, marketingben, politikában, vagy terápiás megoldásokban biometrikus és elemzett adatok segítségével az egyénre visszavezetetett azonosítás által).
- Kihasználják a specifikus sebezhető csoportokat (fizikai vagy mentális fogyatékosság).
- Olyan biometrikus rendszerek, amelyeket közhatalmak vagy azok nevében társadalmi pontozási célokra használhatók.
- „Valós idejű" távoli biometrikus azonosítási rendszerek nyilvánosan hozzáférhető helyeken a rendfenntartási célokra, kivéve néhány korlátozott és szabályozott esetet.

Magas kockázat – Szabályozott magas kockázatú biometrikus rendszerek

Amelyek káros hatást gyakorolnak az emberek biztonságára vagy alapvető jogaira. Megkülönböztethető két kategória a magas kockázatú biometrikus rendszerek között.

Rendszerek, amelyek biztonsági komponenseként működnek egy termék részeként, vagy az EU egészségügyi és biztonsági harmonizációs jogszabályai alá tartoznak (például játékok, légi közlekedés, autók, orvostechnikai eszközök, lift).

Rendszerek, amelyeket nyolc konkrét területen alkalmaznak.

- Biometrikus azonosítás és kategorizáció.
- Kritikus infrastruktúra kezelése és üzemeltetése.
- Oktatás és szakmai képzéssel kapcsolatos rendszerek.
- Foglalkoztatás, munkaerő-menedzsment és az önfoglalkoztatáshoz való hozzáférés.
- Az alapvető magán- és közszolgáltatásokhoz és előnyökhöz való hozzáférés.
- Rendfenntartás.
- Migráció, menedékjog és határellenőrzési menedzsment.
- Igazságszolgáltatás és demokratikus folyamatok adminisztrációja.

Minden ilyen magas kockázatú biometriai azonosítási rendszernek meg kellene felelnie egy szabályrendszernek, amely magában kell foglalja az alábbi követelményeket.

Előzetes megfelelőségi értékelési követelmény. A magas kockázatú biometriai rendszerek szolgáltatóinak regisztrálniuk kellene rendszereiket egy Európai Unió-szerte irányított adatbázisban (amit például az MI-szabályozás mintájára az Európai Bizottság kezelhet), mielőtt piacra dobhatnák vagy szolgáltatásba helyezhetnék azokat. A már meglévő termékbiztonsági jogszabályok által szabályozott bármilyen biometrikus vagy MI alapú termék és szolgáltatás azokba a már meglévő harmadik fél által történő megfelelőségi keretekbe tartozik, amelyek már érvényesek (például az orvostechnikai eszközök esetén). Azoknak a magas kockázatú rendszereket szolgáltatóknak, akiknek terméke jelenleg nem esik az EU szabályozása alá, saját megfelelőségi értékelést (önértékelést) kell készíteniük, amely bizonyítja, hogy megfelelnek az új követelményeknek. A biometrikus azonosításra használt magas kockázatú MI-rendszereknek kell megfelelniük egy „bejelentett szervezet" által végzett megfelelőségi értékelésnek.

Egyéb követelmények: az ilyen magas kockázatú rendszereknek számos követelménynek kell megfelelniük, különösen a kockázatkezelés, tesztelés, műszaki robusztusság, adatképzés és adatirányítás, átláthatóság, emberi felügyelet és kiberbiztonság területén. Ebben az összefüggésben a magas kockázatú rendszerek szolgáltatóinak, importőreinek, forgalmazóinak és felhasználóinak többféle kötelezettségnek kellene eleget tenniük. Az EU-n kívüli szolgáltatóknak szüksége lehet egy azonosított képviselőre az EU-ban, hogy (többek között) biztosítsák a megfelelőségi értékelést, létrehozzák a piaci monitorozási rendszert és szükség esetén korrekciós intézkedéseket tegyenek.

Arcfelismerés: az MI technológiai fejlődése hajtja az olyan biometrikus megoldások, mint az arcfelismerési eljárások (Facial Recognition Technology, FRT) felhasználását, amelyeket magánszemélyek vagy közhatalmak alkalmaznak ellenőrzésre, azonosításra és kategorizálásra. Az MI-rendszerek alkalmazása elkezdődött, beleértve az arcfelismerési technológiákat is, a magán- vagy közhatalmak által történő verifikációs, azonosítási és kategorizálási célokra. A tervezett MI-szabályozás, a már alkalmazott jogszabályokon túl (például adatvédelem és diszkriminációmentesség), új szabályokat javasol az FRT-k számára, és ezeket megkülönbözteti a „magas kockázatú" vagy „alacsony kockázatú" használati jellemzőik szerint. A valós idejű arcfelismerési rendszerek használata nyilvánosan hozzáférhető helyeken a rendfenntartási célokra tilos lenne, hacsak a tagállamok nem engedélyezik őket fontos közrendvédelmi okokból, és ehhez megfelelő bírósági vagy közigazgatási határozatokat hoznak. Számos más FRT, amelyet nem rendfenntartási célokra használnak (például határellenőrzés, piacterek, tömegközlekedés és akár iskolák), engedélyezhető lenne a biztonsági követelmények teljesítése és egy megfelelőségi értékelés esetén.

Korlátozott kockázat: átláthatósági kötelezettségek

A „korlátozott kockázatot" prezentáló rendszerek, mint például az emberekkel interakcióba lépő alkalmazások (például chatbotok), érzelemfelismerő rendszerek, biometrikus kategorizáló rendszerek, valamint az olyan MI megoldások, amelyek kép-, hang- vagy videótartalmat generálnak vagy manipulálnak (például deepfake-ek), csak korlátozott átláthatósági kötelezettségek alá esnének.

Alacsony vagy minimális kockázat: nincsenek kötelezettségek

Minden más, csak alacsony vagy minimális kockázatot prezentáló biometrikus azonosítást végző rendszer fejleszthető és használható lenne az EU-ban anélkül, hogy megfelelne bármilyen további (az eddigieken túlmutató) jogi kötelezettségnek. Azonban a javaslat célja, hogy az irányelvek létrehozásával ösztönzve legyenek a nem magas kockázatú rendszerek szolgáltatói, hogy önkéntesen alkalmazzák a magas kockázatú rendszerek kötelező követelményeit.

Ugyanakkor a polgári jogi szervezetek az arcfelismerés és egyéb biometrikus adatok indokolatlan vagy önkényes célú használatának betiltását követelik a nyilvános vagy nyilvánosan hozzáférhető helyeken, valamint korlátozásokat szorgalmaznak az MI-rendszerek használata tekintetében, beleértve a határellenőrzést és az előrejelző rendőrségi tevékenységeket. Az AccessNow úgy véli, hogy a tiltott MI-gyakorlatokra vonatkozó rendelkezések túl homályosak, és szélesebb körű tilalmat javasol az MI alkalmazására az emberek fiziológiai, viselkedési vagy biometrikus adatok alapján történő kategorizálására, az érzelmek felismerésére, valamint az ilyen technológiák veszélyes használatára a rendőrségi munka, migráció, menedékjog és határkezelés kontextusában. Ugyanakkor erősebb hatásvizsgálati és átláthatósági követelményeket követelnek. Az Európai Vállalkozások Szövetsége hangsúlyozza (URL7), hogy általános bizonytalanság van az MI értékláncában (fejlesztők, szolgáltatók és az MI-rendszerek felhasználói) megjelenő különböző résztvevők szerepével és felelősségével kapcsolatban. Ez különösen kihívást jelent azoknak a vállalatoknak, amelyek általános célú alkalmazásprogramozási interfészeket vagy nyílt forráskódú MI-modelleket biztosítanak, amelyek nem kifejezetten nagy kockázatú MI-rendszerekhez szántak, de harmadik felek által olyan módon használják őket, amelyet nagy kockázatúnak lehet tekinteni. Azt is szorgalmazzák, hogy a „nagy kockázatú" meghatározását a mérhető kár és a potenciális hatás alapján kellene újradefiniálni. Az AlgorithmWatch javasolja (URL8), hogy a konkrét szabályok alkalmazhatósága nem függhet a technológia típusától, hanem annak egyénekre és a társadalomra gyakorolt hatásától kellene függenie.

Új szabályokat követelnek, amelyek az MI-rendszerek hatása alapján vannak meghatározva, és ajánlják, hogy minden üzemeltető végezzen hatásvizsgálatot, amely esetenként értékeli a rendszer kockázati szintjeit.

Összefoglalás

Összefoglalt véleményünk, hogy – a GDPR szabályzaton túlmenően – a mesterséges intelligencia szabályozásával, annak a személyes adatokra vonatkozó adatkezelési irányelveivel párhuzamosan, megfelelő szabványokat kell kidolgozni a különféle forrásból származtatott biometrikus adatok tárolására és felhasználására, amely magában foglalja a kategorizálásból és a következtetésekből előállított, elemzett és feldolgozott adatokat is. A szabványok kifejezetten biometriára vonatkozó kidolgozásával, a meglévő szabványok átdolgozásával és frissítésével megteremthető lenne egy olyan, kifejezetten biometrikus azonosítási megoldásokra vonatkozó, egyszerűsített auditálható folyamat, mely által garantálható a biometrikus adatok védelme, egyúttal csökkenhet a kockázat is. Lehetővé válik a kockázatokkal arányos intézkedések kidolgozása, és ami még fontosabb, a felhasználók kockázatokkal arányos tájékoztatása hozzájárulna a biometria elterjedéséhez. Az MI-szabályozás többszörösen összefügg a biometrikus azonosítással, így a jogalkotók egyik legfőbb törekvése a szabályozási összhang kialakítása. Ezen stratégiák és szabályzatok célja a teljes folyamatláncon végigfutó szabályozás, együttműködés és információcsere kialakítása a gyártók, jogalkotók és szakmai döntéshozók, kormányzati és hatósági szervek között. A magas szintű döntéselőkészítő dokumentumok és tanulmányok kiemelt témája az oktatás erősítésének fontossága, mely jelentősen hozzájárul a biometrikus megoldások elterjedéséhez, hiszen, ha érti a felhasználó a kockázatokat és nem fél a nem megfelelő adatkezeléstől, mert biztosítva látja jogait és biometrikus adatainak megfelelő védelmét és felhasználását, akkor kevésbé ellenzi a technológiát ebből a szempontból.

Felhasznált irodalom

Ahmad, Z., Ajmal, M., Ahmad, F., Chaudary, M. H., & Naseer, M. (2018). Comparative analysis of biometric recognition techniques. *Bahria University Journal of Information and Communication Technologies, 11*(1), 21–30.

Balla J. (2019). *A biometrikus adatokat tartalmazó úti és személyazonosító okmányok biztonságnövelő hatása a határ-, illetve közbiztonság alakulására*. Dialóg Campus Kiadó.

Crisan, S. (2016). A novel perspective on hand vein patterns for biometric recognition: Problems, challenges, and implementations. In R. Jiang, S. Al-Maadeed, A. Bouridane, & P. Crookes (Eds.), *Biometric security and privacy: Opportunities & challenges in the Big Data era* (pp. 21–49). Springer. https://doi.org/10.1007/978-3-319-47301-7_2

Harakannanavar, S. S., Renukamurthy, P. C. & Raja, K. B. (2019). (2019). *Comprehensive study of biometric authentication systems, challenges and future trends*. *International Journal of Advanced Networking and Applications, 10*(4), 3958–3968. https://doi.org/10.35444/IJANA.2019.10048

Jain, A. K., Ross, A. A., & Nandakumar, K. (2011). *Introduction to Biometrics*. Springer. https://doi.org/10.1007/978-0-387-77326-1

Karimi, Z., Najafabadi, S. A., Nezhad, A. R., & Ahmadi, F. (2022). A big survey on biometrics for human identification. In Saba, T., Rehmen, A. & Roy, S. (Eds.), *Prognostic models in healthcare: AI and statistical approaches* (pp. 305–325). Springer. https://doi.org/10.1007/978-981-19-2057-8_14

Markowitz, J. (2000). *Voice biometric*. *Communications of the ACM, 43*(9), pp. 66–73. https://doi.org/10.1145/348941.348995

Őszi A. (2019). *A biometrikus azonosítási rendszerek helye és szerepe az e-kereskedelemben* (PhD-értekezés). Óbudai Egyetem. http://dx.doi.org/10.13140/RG.2.2.12200.14088

Őszi, A., & Kovács, T. (2011). *Theory of the biometric-based technology in the field of e-commerce*. In *Proceedings of the 12th IEEE International Symposium on Computational Intelligence and Informatics (CINTI 2011)*. Óbuda University. https://doi.org/10.1109/CINTI.2011.6108570

Peña, A., Morales, A., Serna, I., Fierrez, J., & Lapedriza, A. (2021). Facial expressions as a vulnerability in face recognition. In *2021 IEEE International Conference on Image Processing (ICIP)* (pp. 2988–2992). IEEE. https://doi.org/10.1109/ICIP42928.2021.9506444

Ratha, N. K., Connell, J. H., & Bolle, R. M. (2001). *An analysis of minutiae matching strength*. In Bigün, J. & Smeraldi, F. (Eds.), *Audio- and video-based biometric person authentication* (pp. 223–228). Springer. https://doi.org/10.1007/3-540-45344-X_32

Srivastava, H. (2013). *A comparison based study on biometrics for human recognition*. *IOSR Journal of Computer Engineering, 15*(1), 22–29. https://doi.org/10.9790/0661-1512229

Tripathi, K. P. (2011). *A comparative study of biometric technologies with reference to human interface*. *International Journal of Computer Applications, 14*(5), 10–15. https://doi.org/10.5120/1842-2493

Wendehorst, C., & Duller, Y. (2021). *Biometric recognition and behavioural detection* (European Parliament Study No. 696968). European Parliament. https://www.europarl.europa.eu/RegData/etudes/STUD/2021/696968/IPOL_STU(2021)696968_EN.pdf

Yan, Z., Lv, S., Zhang, Y., Zhu, H., & Sun, L. (2019). *Remote fingerprinting on internet-wide printers based on neural network*. In *2019 IEEE Global Communications Conference (GLOBECOM)* (pp. 1–6). IEEE. https://doi.org/10.1109/GLOBECOM38437.2019.9014144

Zhang, D., & Lu, G. (2013). *3D biometrics: Systems and applications*. Springer. https://doi.org/10.1007/978-1-4614-7400-5

A cikkben szereplő online hivatkozások

URL1: *White Paper on Artificial Intelligence: A European approach to excellence and trust.* https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52020DC0065

URL2: *European Parliament and the Council: COM(2018) 795 Coordinated Plan on Artificial Intelligence.* https://ec.europa.eu/transparency/documents-register/detail?ref=COM(2018)795&-lang=en

URL3: *COM(2021) 206 final, 2021/0106 (COD), Proposal for a Regulation laying down harmonised rules on artificial intelligence (Artificial Intelligence Act).* https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52021PC0206

URL4: *IDEMIA cements its biometric technologies leadership in the latest NIST rankings.* https://www.idemia.com/press-release/idemia-cements-its-biometric-technologies-leadership-latest-nist-rankings-2023-09-07

URL5: *European Commission, Tabula Rasa project, Research on vulnerabilities of biometric systems.* https://ec.europa.eu/commission/presscorner/api/files/document/print/en/memo_13_924/MEMO_13_924_EN.pdf

URL6: *European Parliament, Artificial Intelligence Act, COM(2021)206 21.4.2021 2021/0106 (COD).* https://www.europarl.europa.eu/RegData/etudes/BRIE/2021/698792/EPRS_BRI(2021)698792_EN.pdf

URL7: *Joint Letter on the European Commission's Proposal for an AI Act.* https://enterprisealliance.eu/wp-content/uploads/2021/10/Joint-Letter-on-AI-Proposal.pdf

URL8: *Draft AI Act: EU needs to live up to its own ambitions in terms of governance and enforcement.* https://algorithmwatch.org/en/wp-content/uploads/2021/08/EU-AI-Act-Consultation-Submission-by-AlgorithmWatch-August-2021.pdf

URL9: *COM(2018) 237 final, EU AI strategy.* https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52018DC0237&from=EN

URL10: *International standard, IEC/FDIS 31010:2009.* https://www.iso.org/standard/51073.html

Alkalmazott jogszabályok

Az Európai Parlament és a Tanács (EU) 2016/679 rendelete – az egyéneknek a személyes adatok kezelésével kapcsolatos védelméről és az ilyen adatok szabad áramlásáról, valamint a 95/46/EK irányelv hatályon kívül helyezéséről

Az Európai Parlament és a Tanács (EU) 2016/680 irányelve – a bűnüldözésben érvényesítendő adatvédelemről, valamint a 95/46/EK irányelv hatályon kívül helyezéséről

Az Európai Parlament és a Tanács (EU) 2018/1725 rendelete – az uniós intézményekre és szervekre alkalmazandó személyes adatok védelméről, valamint a 45/2001/EK és a 46/95/EK rendelet hatályon kívül helyezéséről

Az Európai Parlament és a Tanács [2021/0106 (COD)] rendelete – a közvetlen hatályú szabályok megállapításáról a MI-re vonatkozó harmonizált előírások alapján

A cikk APA szabály szerinti hivatkozása

Ujhegyi P. & Őszi A. (2025). A biometrikus azonosítás és az MI összefüggései, valamint kockázatértékelési lehetőségei. *Belügyi Szemle*, *73*(5), 977–999. https://doi.org/10.38146/BSZ-AJIA.2025.v73.i5.pp977-999

Nyilatkozatok

Összeférhetetlenség

A szerzők nem jelentettek összeférhetetlenséget.

Finanszírozás

A szerzők nem kaptak pénzügyi támogatást a kutatáshoz, a szerzőséghez és/vagy a cikk publikálásához.

Etikai nyilatkozat

Az adatokat kérésre rendelkezésre bocsátják.

Levelező szerző

A cikk levelező szerzője Ujhegyi Péter, aki az ujhegyi.peter@uni-obuda.hu e-mail címen érhető el.