HADMÉRNÖK
BIZTONSÁGTECHNIKA

18. évfolyam (2023) 1. szám 5–16.
DOI: 10.32567/hm.2023.1.1

Bak Gerda,[1] Őszi Arnold,[2] Kovács Tibor[3]

A biometrikus azonosítás megítélése – 2. rész

Assessment of Biometric Identification – Part II

Dr. Kovács Tibor emlékére ajánljuk.

Napjainkban egyre több helyen találkozhatunk a biometrikus azonosítás különböző módjaival, hiszen jelen van az okostelefonokban, illetve számos vállalkozás is alkalmazza, felismerve annak előnyeit.

Jelen tanulmány azt hivatott felmérni, hogy a felhasználók körében a biometrikus azonosításról milyen vélemények alakultak ki, illetve miként vélekednek ezekről a módszerekről. A kutatás jelentősége abban rejlik, hogy 2006-ban és 2014-ben szintén az Óbudai Egyetem keretein belül már lezajlott két hasonló céllal megfogalmazott kutatás, amelyet a jelen kutatás során igyekeztünk folytatni, valamint tovább vinni.

A *második rész* a megkérdezettek biometrikus azonosításhoz való viszonyát és a rendszerek elfogadottságát mutatja be. Az eredmények alapján elmondható, hogy a biometrikus azonosítás kapcsán a felhasználók ismeretei bővítésre szorulnak, mivel még mindig sokan csak használják ezeket a technológiákat a hozzá tartozó tudásanyag és tudatosság nélkül.

Kulcsszavak: biometrikus azonosítás, megítélés, elfogadottság, 2006, 2014, 2021

Nowadays, biometric identification is becoming more and more common, as it is present in smartphones and is also used by many businesses that recognise its benefits.

This study aims to assess the perceptions and opinions of users on biometric identification. The significance of the research lies in the fact that two studies with similar aims were conducted in 2006 and 2014, also at Óbuda University, which we tried to continue and further develop in the present research.

[1] Óbudai Egyetem Biztonságtudományi Doktori Iskola, e-mail: bak.gerda@uni-obuda.hu
[2] Óbudai Egyetem Bánki Donát Gépész és Biztonságtechnikai Mérnöki Kar, e-mail: oszi.arnold@bgk.uni-obuda.hu
[3] Óbudai Egyetem Bánki Donát Gépész és Biztonságtechnikai Mérnöki Kar, e-mail: kovacs.tibor@bgk.uni-obuda.hu

The second part looks at respondents' attitudes towards biometric identification and acceptance of the systems. Based on the results, it can be said that the users' knowledge of biometric identification needs to be expanded, as many people still simply use these technologies without the corresponding knowledge and awareness.

Keywords: biometric identification, perception, acceptance, 2006, 2014, 2021

Bevezetés

A biometrikus azonosítás iránti igény az elmúlt években jelentős mértékben megsokszorozódott, a digitális személyazonosítási rendszerek piaci értéke a következő évek során a kétszeresére nő, ami közel 50 milliárd dollárt jelent világszerte, továbbá globálisan a biometrikus rendszerekre költött összeg 2025-re elérheti a 68,6 milliárd dollárt.[4]

A biometrikus rendszerek adta kényelemnek azonban számos kockázata is van, ilyen például, hogy az egyes szenzorok megtéveszthetők, az egyén biometrikus adatait tároló adatbázis, vagy akár a hálózat szintén célpontja lehet a támadóknak.[5] Az IBM[6] online felméréséből kiderül, hogy bár fontos a megkérdezettek számára a kényelem a különböző applikációkba és alkalmazásokba való bejelentkezés során, azonban a biztonságot fontosabbnak ítélik meg. Ennek kapcsán az is kiderült, hogy a megkérdezettek 67%-ának nem okoz gondot valamilyen biometrikus azonosítási módot alkalmazni, illetve 44%-uk az ujjnyomatot mint azonosítási módot tekinti a legbiztonságosabbnak, valamint a pénzügyi alkalmazások kapcsán tekintik igazán lényegesnek a biztonságot, ezzel szemben a közösségimédia-applikációk esetében a kényelmes, gyors bejelentkezés a fő szempont.

A digitális technológia fejlődésével és használatával számos információ keletkezik, valamint tárolódik a számítógépeken, telefonokon, vagy akár az interneten egyetlen nap leforgása alatt is. Ezeket a tartalmakat pedig érdemes, sőt ajánlott gondosan őrizni, jelszavakkal, azonosítókkal védeni. A jelenlegi technológiát tekintve három azonosítási, hitelesítési módot különböztetünk meg, illetve létezik egy negyedik is, azonban az csak az ötvözete az első két módnak:[7]

- amit a felhasználó tud (jelszó, PIN-kód);
- amivel a felhasználó rendelkezik (kártya, kulcs);
- ami az egyén testi tulajdonságaihoz kapcsolódik (írisz, DNS, ujj[le]nyomat, retina).

Jelen kutatás a következőkben a felsorolásban az utolsó, vagyis az egyén fizikai sajátosságaival foglalkozó azonosítási módra terjed ki.

Biometrikus azonosítás

A számos biometrikus jellemző, például ujj(le)nyomat, írisz vagy arc, egyszerű és mégis szinte lemásolhatatlan, azonban az egyes rendszerek pontossága az adott biometrikus

[4] Liu 2021.
[5] Földesi 2015a; Rui–Yan 2019; Dargan–Kumar 2020.
[6] IBM 2018.
[7] Datta et al. 2020; Szűcs–Őszi–Kovács 2020.

jellemző egyediségétől is függ, valamint a rendszer megbízhatóságától is.[8] Ahogy azt az előbb említettük, a biometrikus rendszerek eltérő megbízhatóságúak, ami nagyban függ a rendszer beállításaitól (például szenzor minősége, típusa, adatbázis mérete, minta-összehasonlítás módja)[9] és a környezeti tényezőktől (hőmérséklet, fényviszonyok, zajok) is.[10]

A biometrikus azonosítás pontosságánál maradva érdemes megemlíteni két mutatót, amelyek a FAR (false accepting rate, téves elfogadási arány) és a FRR (false rejecting rate, téves elutasítási arány).[11]

Nemcsak a rendszerekkel szemben, hanem a biometrikus azonosítójegyekkel szemben is számos követelménynek kell teljesülnie, ilyen követelmények az állandóság, egyediség, egyetemesség, megszerezhetőség, teljesítmény, elfogadottság, megtéveszthetőség és a mérhetőség.[12]

Az 1. táblázat az előbb felsorolt nyolc szempont mentén sebezhetőségük szintjét (M = magas, K = közepes, A = alacsony) mutatja be, valamint hasonlítja össze az egyes biometrikus azonosító jegyeket a teljesség igénye nélkül, a szerzők belátása szerint.

1. táblázat: A biometrikus azonosítási módszerekkel szemben támasztott követelmények és a sebezhetőségi szintjük

Követelmény/ azonosító	Fül	Arc	Ujj(le)-nyomat	Járás	Írisz	Kézgeo-metria	Tenyér-erezet	Retina	Aláírás	Hang	DNS
Egyetemesség	M/K	M	K	K/M	M	K/M	K	M	A	K	M
Egyediség	K	A/K	M	A/K	M	K	K	M	A	A	M
Állandóság	M	K	M	A/K	M	K/A	K	K/M	A	A	M
Megszerezhetőség	K	M	K	M	K/M	M	K	A/K	M	K	A
Teljesítmény	K	A	M	M/A	K/M	K	K	M	A/K	A	A/M
Elfogadottság	M	M	K	M/K	A/K	K	K	A	M	M	A
Megtéveszthetőség	K	M	K	K	A	K	A	A	M	M	A
Mérhetőség	M	M	M	K	K	M	M	M	K	A	M

Forrás: a szerzők szerkesztése Sabhanayagam – Prasanna Venkatesan – Senthamaraikannan 2018 és Dargan–Kumar 2020 alapján

A biometrikus azonosítási módok elfogadottsága

A biometrikus azonosítási módok megjelenése óta számos tanulmány foglalkozik ezeknek a rendszereknek a felhasználók oldaláról érkező visszajelzéseivel, azok

[8] Földesi 2015b.
[9] Őszi 2019.
[10] Fialka–Kovács 2016; Neal–Woodard 2016.
[11] Kovács 2010; Kovács–Milák–Otti 2012.
[12] Kovács–Milák–Otti 2012.

elfogadottságával, illetve azok megítélésével a bűnügyi nyomozásoktól az utazásokon át egészen a mobileszközökre vonatkozóan.[13]

Verena Zimmermann és Nina Gerber tanulmánya is rávilágít arra, hogy a biometrikus azonosítási módok népszerűek a felhasználók körében, annak ellenére, hogy a már jól ismert jelszó használatát preferálja a többség. A kutatásukban a jelszó volt a leggyakrabban említett azonosítási technika. Néhány korábbi tanulmány alapján azonban a biometrikus rendszereket tekintve is megállapítható egy lista, amelyen az ujjlenyomat- és az íriszazonosítás az első helyeken szerepelnek.[14] Steven Furnell és Konstantinos Evangelatos felmérésében például az ujjlenyomatot és az íriszszkennelést értékelték a legmegbízhatóbbnak,[15] Sevasti Karatzouni és munkatársai pedig az ujjlenyomatot találták a legnépszerűbb választásnak az okostelefonokon való biometrikus alkalmazáshoz.[16]

A biometrikus technológia felhasználók általi megítélését vizsgálva nem hagyható figyelmen kívül az adott preferáltság mögött álló indíték sem, hiszen a jelszavakat és a biometrikus technológiákat különböző okokra visszavezethetően részesítik előnyben az egyének. Míg a jelszó, amellett hogy mindenki ismeri, nem igényel a felhasználótól semmilyen személyes adatot, amelyet esetlegesen a támadók ellophatnak. Ezzel szemben, akik a biometrikus azonosítást részesítik előnyben, éppen az előbb említett indok miatt teszik, vagyis a felhasználó egyedi személyes adatai révén való azonosítást nehezebben feltörhetőnek vélik. A résztvevők többnyire az adott jellemző egyediségét és hamisíthatatlanságát nevezték meg a biometrikus adatok használatának indokaként. A különböző felhasználói preferenciák feltételezését más tanulmányok eredményei is alátámasztják, amelyek azt mutatják, hogy az emberek összetett, kissé kettősséget mutató véleményt alkotnak a biometriáról. Ezzel kapcsolatban azonban figyelembe kell venni a biometriával való ismeretséget, vagyis akár a személyes tapasztalat, akár a filmekből, sorozatokból szerzett ismeretség is befolyásolhatja a biometrikus azonosítási módok megítélését.[17]

Módszertan

A kutatás során kvantitatív kutatást folytattunk kérdőíves felmérés formájában, amely 2021. október 23. és 2021. december 12. között zajlott, hólabda módszerrel. A kérdőívet online és offline formában is terjesztettük. Összesen 209 teljes és értékelhető kitöltést kaptunk. Az adatok nem tekinthetők semmilyen értelemben reprezentatívnak, illetve elemzésük IBM SPSS 26 programmal történt.

Maga a kérdőív két fő részből tevődött össze: az általános demográfiai és a biometrikus azonosítással kapcsolatos részből. A kérdések zárt, illetve Likert-skála segítségével voltak megválaszolhatók.

[13] Deane et al. 1995; Chau–Stephens–Jamieson 2004; Negri–Borille–Falcão 2019.
[14] Zimmermann–Gerber 2017.
[15] Furnell–Evangelatos 2007.
[16] Karatzouni et al. 2011.
[17] Zimmermann–Gerber 2017.

A kutatás legelején négy fő kérdés fogalmazódott meg, amelyek a következőkben láthatók.

Kutatási kérdések:

1. Mely biometrikus azonosítási rendszereket használják a hétköznapokban az emberek az okostelefonjaikon?
2. Mennyire elfogadottak ezek a rendszerek a hétköznapokban?
3. Van-e különbség a biometrikus azonosítási rendszerek megítélésében a nemek tekintetében?
4. Miként vélekednek az emberek a biometrikus azonosítási rendszerekről?

Ahogy azt már korábban, illetve az első részben említettük, a kutatás jelen része a második, harmadik és negyedik kutatási kérdéssel foglalkozik.

A minta bemutatása

A kérdőív kitöltőiről nemek szerinti bontásban elmondható, hogy az erősebbik nem dominált, főként Z generációs fiatalok töltötték ki, akik jelenleg is a felsőoktatásban tanulnak, illetve többségében a fővárosban laknak. A kitöltők leíró statisztikai jellemzőit a 2. táblázat foglalja össze.

2. táblázat: A kérdőív kitöltőinek leíró statisztikája (n = 209)

		N	%
Nem	Férfi	125	59,8
	Nő	84	40,2
Generáció	Z generáció	113	54,1
	Y generáció	70	33,5
	X generáció	23	11,0
	Baby boom	3	1,4
Lakhely	Főváros	89	42,6
	Megyeszékhely	40	19,1
	Város	53	25,4
	Község	16	7,7
	Falu	11	5,3
Iskolai végzettség	Befejezett 8 osztály	1	0,5
	Érettségi	47	22,5
	Szakmunkásképző	5	2,4
	BSc	54	25,8
	MSc	27	12,9
	PhD	5	2,4
	Jelenleg is felsőoktatásban tanul	66	31,6
	Posztgraduális	1	0,5
	Egyéb	3	1,4

Forrás: a szerzők szerkesztése a minta adatai alapján

Eredmények

A kérdőív biometrikus azonosítási rendszerek elfogadottságát vizsgáló része előtt négy olyan kérdést tettünk fel a kitöltőknek, amelyek egyrészt átvezetésül szolgálnak a mélyebb kérdésekhez, másrészt a segítségükkel általános képet kaphatunk a felhasználók biometrikus azonosítási módszerekkel kapcsolatos véleményéről és hozzáállásáról. Az említett kérdések közül az első kivételével ötfokozatú Likert-skálán kellett a válaszadóknak jelölniük a válaszukat. Ez a négy kérdés a következő:

- Kelt-e Önben valamilyen averziót, ha írisz- vagy retinavizsgálatos beléptetést kell használnia?
- Általában mennyire tartja korszerűnek a biometrikus azonosításon alapuló beléptetési lehetőséget?
- Ön szerint mennyire könnyű/egyszerű egy biometrikus rendszer használata?
- Mennyire találja gyorsnak a biometrikus azonosítási folyamatot?

A további három átvezető kérdés esetében az ötfokozatú Likert-skála értékei a következő módon alakultak: 1 – nem tartják korszerűnek, könnyűnek, illetve gyorsnak a biometrikus rendszerek alkalmazását, a skála másik végén elhelyezkedő 5 – nagyon korszerű, könnyű és gyors e rendszerek alkalmazása. Az említett kérdésekre adott válaszok leíró statisztikáját foglalja össze a 3. táblázat. Amint az a táblázatból leolvasható, a kitöltők válaszai alapján a biometrikus rendszerekről alkotott vélemények nagyon pozitívak, hiszen általánosságban korszerűnek, könnyen használhatónak és gyorsnak gondolják őket. Az 1–5-ig terjedő skálán a válaszadók átlagosan 4-es értékkel jelölték a biometrikus rendszereket, az adott három tényező alapján. A három tényező közül a legjobb értékelést a rendszer korszerűsége kapta, amelynek átlaga 4,39 (SD = 0,707), a legrosszabbat pedig a rendszer tempója, amelynek az átlaga 4,03 (SD = 0,901).

3. táblázat: A biometrikus azonosítási rendszerek általános megítélése (n = 209)

	Átlag	**Medián**	**SD**
A biometrikus beléptetés korszerűsége	4,39	5,00	0,707
A biometrikus rendszer használatának egyszerűsége	4,09	4,00	0,866
A biometrikus rendszer használatának gyorsasága	4,03	4,00	0,901

Forrás: a szerzők szerkesztése a minta adatai alapján

Az előbbi kérdések kapcsán megvizsgáltuk, hogy a nemek tekintetében van-e eltérés a biometrikus rendszerek megítélésében. Az eredmények fényében elmondható, hogy az elvégzett khí-négyzet-elemzés csak a biometrikus azonosítási rendszerek gyorsaságát tekintve mutat szignifikáns eltérést ($p = 0,018$) a nemek tekintetében, a másik két szempontot, azaz a korszerűséget ($p = 0,716$) és az egyszerűségüket ($p = 0,330$)

tekintve azonban nincs jelentős különbség. Ez azt jelenti, hogy az, hogy az egyén melyik nemhez tartozik, nem befolyásolja a biometrikus rendszerek korszerűségéről és használatának egyszerűségéről alkotott megítélését, viszont a rendszer gyorsaságát tekintve azonban már van jelentősége.

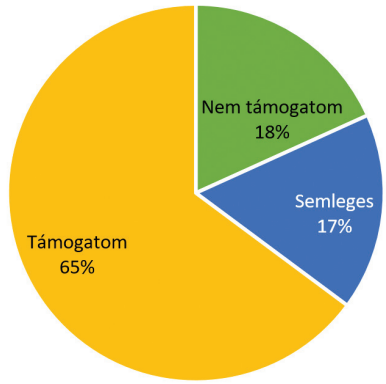
A biometrikus azonosítás kapcsán megfogalmaztunk állításokat és megkérdeztük a kitöltőket, hogy egy ötös Likert-skálán vizsgálva mennyire értenek egyet az egyes állításokkal. A 4. táblázat az ezekre adott válaszokat tartalmazza. Az eredmények tükrében elmondható, hogy a megkérdezettek számára tetszetős módszer, amelyet szívesen használnak, akár a munkahelyen is, illetve a megkérdezetteket nem zavarja a biológiai adataik nyilvántartása, nem sérül általa a személyiségi joguk, valamint nem tartanak a biometrikus azonosítás egészségkárosító hatásától sem. Érdekességként megemlítendő még, hogy akinek tetszenek a biometrikus rendszerek, azok modernnek tartják és szívesen is használnák. Továbbá akik szerint korszerű a biometrikus azonosítás, azok nem félnek az egészségkárosító hatásuktól.

4. táblázat: A biometrikus azonosítás elfogadottsága (n = 209)

A biometrikus azonosítás…	**Átlag**	**Medián**	**SD**
Sérti a személyiségi jogaimat.	2,61	3,00	0,677
Mint módszer tetszik, szívesen használom.	2,57	3,00	0,731
Félek az esetleges egészségkárosító hatásaitól.	2,78	3,00	0,543
A munkahelyemen is szívesen használnék hasonlót.	2,30	3,00	0,832
Zavar a biológiai adataim nyilvántartása.	2,29	3,00	0,857
A legmodernebb rendszer, amivel személyesen találkoztam.	2,64	3,00	0,651
Otthon is szívesen használnám.	2,06	2,00	0,888

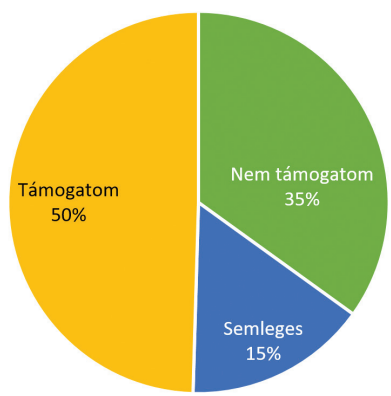
Forrás: a minta adatai alapján a szerzők szerkesztése

A biometrikus azonosítással kapcsolatos megítélést szemlélteti az előzőleg bemutatott állítások összesített formájában a 1. ábra. A kitöltők ötfokú Likert-skála segítségével jelölhették, hogy mennyire értenek egyet az egyes állításokkal. A válaszokat azonban jelen esetben 3 csoportba soroltuk a következő módon: az 1 és 2 értékek a nem értenek egyet csoportot, azok akik a 3-at jelölték, azok a semleges csoportot, a 4 és 5 értékek pedig az egyetértők csoportját alkotják. Látható, hogy a kitöltők 65%-a támogatóan, 17% számára semleges módon és 18% pedig ellenérzéssel viszonyul az általánosan vett biometrikus rendszerek alkalmazásához.



1. ábra: A kitöltők viszonyulása a biometrikus rendszerek alkalmazásához (n = 209)
Forrás: a szerzők szerkesztése a minta adatai alapján

A kutatás zárásaként a kitöltőket a különböző biometrikus azonosítók (elektronikus) adatbázisban való rögzítéséről kérdeztük különböző aspektusok szerint. A kitöltők válaszait ennél a kérdéscsoportnál is csoportosítottuk az előbbi blokkosításnál bemutatott eljárással. A kitöltők viszonyulását a biometrikus adatok általános rögzítéséhez a 2. ábra mutatja be. Az eredmények alapján a megkérdezettek fele támogatja a biometrikus adatok adatbázisban való rögzítését, azonban 35%-uk kifejezetten ellenzi, valamint 15% számára semleges. Az eredményeket tekintve itt is megemlítendő két érdekesség. Egyrészt aki nem szeretné, hogy bármilyen szándékos bűncselekményt elkövető személy ujjlenyomatán kívül további biometrikus adatai (DNS, írisz, érhálózat stb.) is rendőrségi nyilvántartásba kerüljenek, az nem hallott biometrikus azonosítási rendszerekről (22-ből 21 esetben igaz). Másrészt pedig, aki nagyon nem ért egyet azzal, hogy az abúzust (gyermekek szexuális bántalmazása) és szándékos emberölést elkövető egyének DNS-mintája, ujjlenyomata, arcazonosításra alkalmas paraméterei rendőrségi nyilvántartásba kerüljenek, ők mind a fővárosban élnek (6 eset).



2. ábra: Az egyének biometrikus azonosítóinak rögzítési elfogadottsága (n = 209)
Forrás: a szerzők szerkesztése a minta adatai alapján

A 2006., 2014. és 2021. évi eredmények összehasonlítása

Ahogy azt a jelen tanulmány korábbi szakaszában is említettük, 2014-ben, illetve 2006-ban már lefolytattunk két, a jelenlegi kutatáshoz hasonló felmérést, így a következőkben kitérünk a három kutatás eredményeinek összevetésére is.

A kitöltők biometriával kapcsolatos hozzáállása az évek során kis mértékben, azonban negatív irányba változott. A 2006-os felmérés során a megkérdezettek 70%-a, a 2014-es felmérésnél 69%, a 2021-es felmérés pedig 65%-os pozitív, támogatói attitűdöt mutat.

A biometrikus adatok adatbázisban való egyetemleges rögzítése kapcsán azonban pozitív változás látszik, ugyanis 2014-ben – az egyetemistákat tekintve – mindössze 38%-uk vélekedett támogatóan, ezzel szemben a jelenlegi kutatásnál a megkérdezettek 50%-a vélekedett hasonlóan.

A biometrikus eszközök egészségkárosító hatásaitól való félelmek mértéke szinte változatlan maradt az évek során. 2006-ban a megkérdezettek 68%-a egyáltalán nem tartott attól, hogy esetlegesen az egészségükre káros lenne az optikai érzékelővel felszerelt biometrikus azonosítási eszköz használata. 2021-ben a megkérdezettek 69,4%-a vélekedett hasonlóan.[18] Ezt látva továbbra is elmondható, hogy sem 2006-ban, sem 2021-ben nem rendelkeznek a megkérdezettek megfelelő tudással a biometrikus azonosítási eljárásokról.

Mivel a 2006-ban és 2021-ben lefolytatott kutatások konkrétan nem tartalmaztak kérdéseket a kitöltők biometriai ismereteire, viszont 2014-ben igen, így közvetve tudunk csak következtetni az ismeretek, a tudás mértékére az első és az utolsó kutatás kapcsán, amelyek, amint azt az előbbi példa mutatja, hiányosak és felületesek. A 2014-ben lezajlott kutatás eredményei szintén hasonló képet mutatnak, amely szerint a megkérdezettek nagyobbik felének felületes és nem naprakész információi vannak a témával kapcsolatban.[19]

Következtetések

A jelen kutatás eredményei, amely szerint az emberek pozitívan értékelik a biometrikus azonosítási rendszereket, hasonlóságot mutat több nemzetközi kutatással is.[20] Ezen túlmenően az Oliver Buckley és Jason R. C. Nurse által lefolytatott kutatás nemcsak azon a téren kapott a jelen kutatás eredményeihez hasonló eredményeket, mint a biometrikus azonosítási rendszerek pozitív megítélése, hanem a felhasználók biometrikus azonosítással kapcsolatos ismereteiről is.[21] Egy másik tanulmány szerint a turistákat a biometrikus azonosítási rendszerek megléte egy szállodában pozitívan befolyásolja. Ezt azt jelenti, hogy olyan mértékű bizalommal vannak a technológia

[18] Suplicz–Fűzi–Horváth 2006; Földesi 2015a; Földesi–Kovács 2021.
[19] Kovács–Földesi 2015: 26.
[20] Bhagavatula et al. 2015; Buckley–Nurse 2019.
[21] Buckley–Nurse 2019.

felé, hogy biztonságosabbnak ítélik meg azokat a szállodákat, ahol biometrikus technológiát alkalmaz az adott szállás.[22]

A biometrikus rendszerek elfogadottságát tekintve vegyes képet mutatnak az eredmények, amelyek megegyeznek más kutatásokkal,[23] azaz a felhasználók nyitottak az új technológiai megoldásokra,[24] de azoknak a használata és elfogadása nagyban függ a technológia hasznosságától, használatának egyszerűségétől vagy épp nehézségétől, valamint számos olyan tényezőtől is, amelyeket a jelen tanulmányban nem vizsgáltunk.[25]

A kutatás harmadik, egyben utolsó kérdéséhez kapcsolódó eredmény alapján, amely szerint különbség van a biometrikus azonosítási rendszerek megítélésében a nemek tekintetében, az mondható, hogy minimális a különbség, szinte nincs is.

Összefoglalás

Az eredményeket tekintve elmondható, hogy bár a megkérdezettek nagy része pozitívan tekint a biometrikus azonosítási módokra és szívesen is használja azokat, mégis az alacsonyabb szintű tudatosságuk következtében tartanak az adataik központi, nagymértékű tárolásától. A későbbiek során érdemes lehet az e mögött álló indokok feltérképezése is, ezáltal is elősegítve a rendszer megítélésének további növelését.

Az előbbi eredményeket összegezve elmondható, hogy szükséges a tématerület részletesebb és mélyebb megismertetése az egyénekkel, ezzel is növelve a biometrikus rendszerekbe vetett bizalmat, valamint szakszerű felhasználásának elősegítését.

Felhasznált irodalom

Bhagavatula, Rasekhar – Ur, Blase – Iacovino, Kevin – Kywe, Su Mon – Cranor, Lorrie Faith – Savvides, Marios (2015): Biometric Authentication on Iphone and Android: Usability, Perceptions, and Influences on Adoption. In *Proceedings 2015 Workshop on Usable Security,* 8 February, San Diego, CA: NDSS. 1–10. Online:: https://doi.org/10.14722/usec.2015.23003

Buckley, Oliver – Nurse, Jason R. C. (2019): The Language of Biometrics: Analysing Public Perceptions. *Journal of Information Security and Applications,* 47, 112–119. Online: https://doi.org/10.1016/j.jisa.2019.05.001

Chau, Angela – Stephens, Greg – Jamieson, Rodger (2004): *Biometrics Acceptance – Perceptions of Use of Biometrics.* ACIS 2004 Proceedings 28. Online: https://aisel.aisnet.org/cgi/viewcontent.cgi?article=1147&context=acis2004

Dargan, Shaveta – Kumar, Munish (2020): A Comprehensive Survey on the Biometric Recognition Systems based on Physiological and Behavioral Modalities.

[22] Pai et al. 2018.
[23] Otti–Valociková 2019; Semnani-Azad et al. 2019.
[24] Krupp–Rathgeb–Busch 2013.
[25] Tick 2018; Otti–Valociková 2019.

Expert Systems with Applications, 143, 113114. Online: https://doi.org/10.1016/j.eswa.2019.113114

Datta, Priyanka – Bhardwaj, Shanu – Panda, S. N. – Tanwar, Sarvesh – Badotra, Sumit (2020): Survey of Security and Privacy Issues on Biometric System. In *Handbook of Computer Networks and Cyber Security.* Cham: Springer. 763–776. Online: https://doi.org/10.1007/978-3-030-22277-2_30

Deane, Frank – Barrelle, Kate – Henderson, Ron – Mahar, Doug (1995): Perceived acceptability of biometric security systems. *Computers & Security,* 14(3), 225–231. Online: https://doi.org/10.1016/0167-4048(95)00005-S

Fialka, György – Kovács, Tibor (2016): The Vulnerability of Biometric Methods and Devices. *Annals of Faculty Engineering Hunedoara – International Journal of Engineering,* 14(3), 45–48.

Földesi Krisztina (2015a): A biometrikus azonosításhoz kapcsolódó averziók feltárására lefolytatott kutatás. *Magyar Rendészet,* 15(5), 21–35.

Földesi Krisztina (2015b): Paradigmaváltás a biztonságtechnikában – miért alkalmazzunk biometrikus rendszert? *Magyar Rendészet,* 15(3), 37–48.

Földesi Krisztina – Kovács Tibor (2021): Összehasonlító kutatáselemzés a biometrikus személyazonosító-beléptető rendszerek, eljárások 2006. és 2014. évi társadalmi averzív reakcióinak vizsgálatára. *SecureInfo,* 2021. december 10. Online: www.securinfo.hu/wp-content/uploads/2015/06/20150602_osszehasonlito_elemzes_a_biometrikus_szemelyazonosito_rendszerek.pdf

Furnell, Steven – Evangelatos, Konstantinos (2007): Public Awareness and Perceptions of Biometrics. *Computer Fraud & Security,* 2007(1), 8–13. Online: https://doi.org/10.1016/S1361-3723(07)70006-4

IBM (2018): IBM Security: IBM Security: Future of Identity. 2021. december 10. Online: www.ibm.com/downloads/cas/PL9VJ9KV

Karatzouni, Sevasti – Furnell, Steven M. – Clarke, Nathan L. – Botha, Reinhardt A. (2007): Perceptions of User Authentication on Mobile Devices. *Proceedings of the ISOneWorld Conference.* 11–13.

Kovács Tibor (2010): *Biometrikus azonosítás.* PhD-értekezés. Budapest: Óbudai Egyetem.

Kovács Tibor – Milák István – Otti Csaba (2012): A biztonságtudomány biometriai aspektusai. In Gaál Gyula – Hautzinger Zoltán (szerk.): *A biztonság rendészettudományi dimenziói: Változások és hatások.* Pécs: Magyar Rendészettudományi Társaság, 485–496. Online: www.pecshor.hu/periodika/XIII/kovacsti.pdf

Krupp, Alina – Rathgeb, Christian – Busch, Christoph (2013): Social Acceptance of Biometric Technologies in Germany: A Survey. In *2013 International Conference of the BIOSIG Special Interest Group (BIOSIG).* IEEE. 1–5.

Liu, Shanhong (2021): Biometric Technologies – Statistics & Facts. *Statista,* 2021. október 30. Online: www.statista.com/topics/4989/biometric-technologies/#dossierKeyfigures

Neal, Tempestt J. – Woodard, Damon L. (2016): Surveying Biometric Authentication for Mobile Device Security. *Journal of Pattern Recognition Research,* 11(1), 74–110. Online: https://doi.org/10.13176/11.764

Negri, Nathane Ana Rosa – Borille, Giovanna Miceli Ronzani – Falcão, Viviane Adriano (2019): Acceptance of Biometric Technology in Airport Check-in. *Journal of Air*

Transport Management, 81, 101720. Online: https://doi.org/10.1016/j.jairtraman.2019.101720

Otti, Csaba – Valociková, Cyntia (2019): A biztonsági rendszerek felhasználói attitűdje, értékelése és felhasználásának lehetőségei. *Hadmérnök,* 14(1), 32–41. Online: https://doi.org/10.32567/hm.2019.1.3

Őszi Arnold (2019): *A biometrikus azonosítás helye és szerepe az e-kereskedelemben.* PhD-értekezés. Budapest: Óbudai Egyetem.

Pai, Chen-Kuo – Wang, Te-Wei – Chen, Shun-Hsing – Cai, Kun-You (2018): Empirical Study on Chinese Tourists' Perceived Trust and Intention to Use Biometric Technology. *Asia Pacific Journal of Tourism Research,* 23(9), 880–895. Online: https://doi.org/10.1080/10941665.2018.1499544

Rui, Zhang – Yan, Zheng (2019): A Survey on Biometric Authentication: Toward Secure and Privacy-Preserving Identification. *IEEE Access,* 7, 5994–6009. Online: https://doi.org/10.1109/ACCESS.2018.2889996

Sabhanayagam, T. – Prasanna Venkatesan, V. – Senthamaraikannan, K. (2018): A Comprehensive Survey on Various Biometric Systems. *International Journal of Applied Engineering Research,* 13(5), 2276–2297.

Semnani-Azad, Zhaleh – Chien, Shih-Yi – Forster, Yannick – Schuckers, Stephanie – Gan, Houchao: Development of Trust Measure in Biometric Technology. In *Proceedings of the 52nd Hawaii International Conference on System Sciences.* HICSS, 2019. 5797–5804. Online: https://doi.org/10.24251/HICSS.2019.699

Suplicz Sándor – Fűzi Beatrix – Horváth Sándor (2006): Írisz felismerésen alapuló beléptető rendszer által keltett attitűdök és averzív reakciók vizsgálata. In *6. Nemzetközi Mechatronikai és Biztonságtechnikai Szimpózium.* Budapest: Budapesti Műszaki Főiskola.

Szűcs, Kata Rebeka – Őszi, Arnold – Kovács, Tibor (2020): Mobile Biometrics and their Risks. *Hadmérnök,* 15(4), 15–28. Online: https://doi.org/10.32567/hm.2020.4.2

Tick Andrea (2018): Az IT biztonságtudatosság szerepe az e-learning hallgatói használati hajlandóságának TAM modelljében magyar oktatási környezetben – A strukturális egyenlet modellezés. *Hadmérnök,* 13(3), 453–470. Online: https://folyoirat.ludovika.hu/index.php/hadmernok/article/view/3912

Zimmermann, Verena – Gerber, Nina (2017): "If It Wasn't Secure, They Would Not Use It in the Movies" – Security Perceptions and User Acceptance of Authentication Technologies. In *Human Aspects of Information Security, Privacy and Trust. HAS 2017. Lecture Notes in Computer Science.* Cham: Springer. 265–283. Online: https://doi.org/10.1007/978-3-319-58460-7_18