

OTDK-dolgozat

2025

BABEŞ-BOLYAI TUDOMÁNYEGYETEM
KÖZGAZDASÁG- ÉS GAZDÁLKODÁSTUDOMÁNYI KAR

**A BIOMETRIKUS FIZETÉSI MEGOLDÁSOK ELFOGADÁSA ÉS
HASZNÁLATI SZÁNDÉKA A ROMÁNIAI FOGYASZTÓK KÖRÉBEN**

**THE ACCEPTANCE AND WILLINGNESS TO USE BIOMETRIC
PAYMENT SOLUTIONS AMONG ROMANIAN CONSUMERS**

Tîrnăvean Anamaria-Petruța

Konzulens: dr. Alt Mónika-Anetta habilitált egyetemi docens

Kézirat lezárásának dátuma: 2024. május 5.

Kivonat

A technológia egyre nagyobb elterjedésének és rohamos fejlődésének köszönhetően, számos iparág innovatív megoldásokat nyújt a fogyasztók számára. Az elmúlt években a pénzügyi és kereskedelmi szektorok is lényeges átalakuláson mentek keresztül. Az innovatív, folyamatosan fejlődő technológiák új fizetési alternatívákat hoztak létre, átalakítva a fogyasztók fizetési szokásait. Ezen új fizetési lehetőségek közé sorolható a biometrikus fizetési módszer, amely egy gyors és kényelmes fizetési opciót kínálhat fel a fogyasztók számára, egy tenyérérintéssel vagy akár egy mosollyal is végbemehet a tranzakció. A biometrikus fizetési alternatíva egy viszonylag új, innovatív területet képvisel a fizetési módszerek között, valamint kevésbé kutatott terület a romániai piacon. Jelen dolgozat célja megvizsgálni a romániai fogyasztók elfogadását és használati szándékát a biometrikus fizetési alternatívák iránt. Továbbá felmérni ezen fogyasztók használati szándékát, valamint a biometrikus fizetési technológia elfogadási tendenciáját kvantitatív, kérdőíves kutatást végezve. A kutatás eredményei olyan új üzleti lehetőségekre mutatnak rá, amelyek elősegítik a biometrikus fizetési technológiák forgalmazásában és alkalmazásában érdekelt vállalatok döntéshozóit, az új technológia bevezetési szándékát illetően. Emellett hozzájárulnak a biometrikus fizetési megoldások fejlesztéséhez és kialakításához, ezáltal növelve a fogyasztói elégedettséget ezen fizetési lehetőséggel szemben.

Tartalomjegyzék

Bevezetés	1
1. Szakirodalmi áttekintő.....	2
1.1 Bevezetés a biometria szakterületébe	2
1.1.1 Biometrikus jellemzők osztályozása	3
1.2 A biometrikus technológia bemutatása	4
1.2.1 Az autentifikáció működési folyamata	5
1.2.2 Identifikáció és verifikáció.....	6
1.2.3 Adatvédelmi eljárások	7
1.2.4 Biometrikus ismérveket felhasználó rendszerek működése.....	8
1.3 A biometrikus technológia alkalmazása fizetési megoldásként	8
1.3.1 Biometrikus fizetési megoldások működése.....	10
1.4 Innovatív fizetési megoldások használati szándékának kutatásai	11
2. Konceptuális modell és hipotézisek	13
3. Alkalmazott kutatási módszertan	18
3.1 A kutatási módszertan bemutatása, előnyei és hátrányai	19
3.2 A kérdőív felépítése és mérés	20
3.3 Mintavétel és adatgyűjtési folyamat	21
4. Eredmények	22
4.1 Leíró statisztika.....	23
4.2 Hipotézisek tesztelése.....	25
5. Következtetések	28
5.1 A kutatás korlátai	31
5.2 További kutatási lehetőségek	31
5.3 Gyakorlati jelentőség és javaslatok	32
Irodalomjegyzék	34
Mellékletek.....	37

Táblázatok és ábrák jegyzéke

Táblázatok:

Táblázat 1 - A válaszadók demográfiai jellemzői (N=148)	23
---	----

Ábrák:

1 Ábra - Biometrikus regisztrációs (enrollment) folyamat	5
2 Ábra - Konceptuális modell és hipotézisek.....	18
3 Ábra- A válaszadók által használt fizetési módszerek megoszlása (%).....	24
4 Ábra- A konceptuális modell tesztelésének eredménye.....	28

Bevezetés

A technológia rohamos fejlődésének köszönhetően, számos iparági szereplő törekszik, a fogyasztói számára kialakítani a legmegfelelőbb megoldásokat. Az elmúlt években a pénzügyi szektorban is jelentős változások mentek végbe, így jelentősen megváltoztak a fogyasztók fizetési szokásaik.

A romániai fogyasztók körében is egyre jelentősebbé váltak az innovatív fizetési megoldások, a hagyományos megoldásokkal szemben. A biometrikus fizetési megoldások egy új, innovatív fizetési megoldást biztosítanak egy ujjérintés vagy akár egy mosoly segítségével. A biometrikus ismérveken alapuló technológia egyre nagyobb teret nyer, amióta a mobiltelefonok feloldásához is használatos lett, ennek köszönhetően számos felhasználó számára elérhetővé vált ezen technológia. A Mastercard (2021) által végzett kutatás eredményei alapján a romániai felhasználók, 49%-a használt már biometrikus ismérveken alapuló technológiát a bankszolgáltatója által biztosított fizetési alkalmazások bejelentkezéséhez. A jövőre nézve, ezen technológia egyre inkább elterjedtebbé válik, a biztonság, illetve a kényelem érzetnek köszönhetően. Így relevánsnak találom a biometrikus fizetési módszerek használati szándékának és elfogadásának kutatását a romániai fogyasztók körében.

Elsőként a szakirodalom áttekintése és elemzése kerül bemutatásra a téma egy jobb megértése érdekében, majd az innovatív fizetési megoldások területén meglévő kutatások megvizsgálására kerül sor. Továbbá bemutatásra kerül a primer kutatás, valamint a kapott eredmények.

Jelen kutatás eredményei hozzájárulnak a biometrikus fizetési megoldások szakirodalmához, valamint pénzügyi és kereskedelmi szektorban tevékenykedő vállalatok számára nyújtanak hasznos javaslatokat, amelyek implemantálni szeretnék ezen technológiát.

1. Szakirodalmi áttekintő

Jelen fejezet során, bemutatásra kerül általánosan a biometria szakterülete, majd a biometrikus technológia bemutatásának témakörét tárgyalom. Ezt követően a különböző biometrikus fizetési megoldások részletezésére kerül a hangsúly. Legutolsó sorban, az innovatív fizetési megoldások elfogadásának, valamint használati szánékának kutatások eredményei kerülnek összegzésre, beleértve a biometrikus fizetési megoldásokat is.

1.1 Bevezetés a biometria szakterületébe

A biometria szó görög eredetű, amely alapvetőleg két kifejezésre bontható: „bio”, amely életet jelent, valamint „metrics”, amely a mérésre vonatkozik (Babisch, 2012). A biometria tehát az a szakterület, amely az élő szervezetek tulajdonságainak mérésével foglalkozik. Ezen terület magába foglalja az embereket, de kiterjed egyaránt a növények és az állatok jellemzőinek mérésére is (Mróz-Gorgoń et al., 2022). Emellett a biometria azon viselkedésbeli és fiziológiai jellemzők felismerésével foglalkozik, amelyek segítségével megkülönböztethető egy egyén a másiktól (Bolle et al., 2004). Továbbá a biometria ezen ismérvek automatizált felhasználásával is foglalkozik, annak érdekében, hogy meghatározza vagy igazolja egy személy egyedi személyazonosságát (Ogbanufe & Kim, 2018). A biometrikus jellemzők esetében, fontos figyelembe venni az alábbi kritériumokat:

1. Egyetemesség – szinte az összes egyénnek rendelkeznie kell az adott tulajdonsággal
2. Egyediség – a tulajdonság jól megkülönböztethető, az egyén ismérvei jól elhatárolhatóak a többi egyén sajátosságaitól
3. Állandóság – a jellemzőnek idővel, legtöbb esetben állandónak kell lennie
4. Mérhetőség vagy megszerezhetőség – a jellemző legyen könnyen mérhető, leolvasható, valamint felismerhető, ne feltételezzon túl magas költségeket, illetve ne legyen túl időigényes folyamat
5. Teljesítmény – pontosság és gyorsaság
6. Elfogadás – milyen mértékben van elfogadva az emberek által az adott biometrikus jellemző (Babisch, 2012), például vallási, kulturális kérdések, higiénia, komfortérzet (Mróz-Gorgoń et al., 2022)
7. Kijátszás – mennyire egyszerű átverni a rendszert, ezen kritérium fontos elemet jelképez, ugyanis az információk egyre nagyobb értékkel rendelkeznek, továbbá egy jó lehetőséget biztosít arra, hogy az esetleges rendszertámadásokat megelőhessen előzni (Babisch, 2012).

1.1.1 Biometrikus jellemzők osztályozása

Számos olyan megkülönböztethető emberi jellemző létezik, amely eleget tesz a biometria tulajdonságainak és meghatározásának (Kumar & Ryu, 2009). A biometrikus jellemzők alapvetőleg két fő kategóriába sorolhatóak: az első kategória a fiziológiai vagy fizikai ismérvek, a második kategória pedig magába foglalja a viselkedésbeli tulajdonságokat (Mróz-Gorgoń et al., 2022). Sreekumar (2010) kutatásában megemlíti egy harmadik csoportot is, a kombinált biometrikus jellemzők kategóriát.

A fiziológiai vagy fizikai jellemzők, olyan tulajdonságok amelyek egy egyén egyes testrészeinek szerkezetére vonatkoznak, ide tartozik például az ujjlenyomat, a tenyérnyomat, a kezek és a fülek alakja, a szemben található írisz és retina mintázata, az arc geometriája, a vérerek mintázata, illetve a DNS (Mróz-Gorgoń et al., 2022). Ezen fiziológiai jellemzők legtöbb esetben változatlanok maradnak az egyén élete során, kivételt képeznek azok az esetek amikor baleset történik vagy olyan események lépnek fel, amelyek előidéznek ezen ismérvek változását, kopását. A fiziológiai jellemzők veleszületett, statikus tulajdonságok, amelyeket nem befolyásolnak külső tényezők, kivéve az előbbieken említett balesetek és változási folyamatok (Sreekumar, 2010).

A viselkedési jellemzők, olyan ismérvek, amelyek összefüggnek a viselkedéssel, illetve az egyének fejlődési folyamata során alakulnak ki (Mróz-Gorgoń et al., 2022). Ezen jellemzők, bizonyos cselekvések tulajdonságain alapulnak, amelyeket egy adott egyén végez (Sreekumar, 2010), például egy személy járásmódja, a P300 agyhullámok mozgása, vagy a billentyűleütés, a kézírás, az aláírás, a beszédstílus, a hang (az utóbbi négy ismérvtől kettős jelleggel rendelkezik – egyaránt fiziológiai és viselkedési) stb. (Mróz-Gorgoń et al., 2022; Sreekumar, 2010). A cselekvések egy adott időkeretbe helyezhetőek, a cselekvés megkezdési pillanata, illetve a cselekvés befejezésének pillanata, világos, jól meghatározott momentum. Bármely viselkedési jellemző, amely az adott időkeretben kerül mérésre biometrikus mintát alkothat. A viselkedési biometriát dinamikusság jellemzi, az idő előrehaladtával változhat. Emellett ezen tulajdonságokat különböző külső tényezők is nagymértékben befolyásolhatnak, mint például az oktatás és az egyén környezete. A kézírás esetében, például egy fontos befolyásoló tényező az iskolai környezet, az oktatás, valamint az író sajátos írási stílusa, amely idővel, az életkorral változhat (Sreekumar, 2010).

Valamely biometrikus adatokra egyaránt jellemzőek fizikai, illetve viselkedésbeli tulajdonságok. Ezen eseteket kombinált biometrikus jellemzőknek nevezik. A beszédfelismerés tipikusan egy kombinált jellegű biometrikus ismérvtől, ugyanis egyaránt

tartalmaz fiziológiai elemeket, mint például az orrüreg, illetve a hangszálak. Ugyanakkor tartalmaz viselkedési jellemzőket is, mint például a beszélő kiejtése, akcentusa és hangsúlya. Az utóbbi tulajdonságokat különböző környezeti tényezők folyásolhatják be, mint például a kapott oktatás, valamint a környezet, a település ahol az adott egyén felnőtt, élt (Sreekumar, 2010).

Az előbbiekben említett kategóriákba tartozó biometrikus tulajdonságok csoportosítását, példákkal ellátva a mellékletekben található Táblázat 1 (Biometrikus jellemzők osztályozása) foglalja össze.

1.2 A biometrikus technológia bemutatása

Liébana-Cabanillas et al. (2024) megközelítése szerint „A biometrikus rendszer egy olyan mintafelismerő rendszer, amely egy személytől biometrikus adatokat vesz fel, majd ezen adatokból kinyer egy sor jellemzőt, és ezeket a jellemzőket összehasonlítja az adatbázisban lévő mintákkal, tulajdonságokkal” (Liébana-Cabanillas et al., 2024, 2. o.). Ezen technológia használata segítséget nyújt az egyének személyazonosságának hitelesítésében, három típusú jellemző alapján:

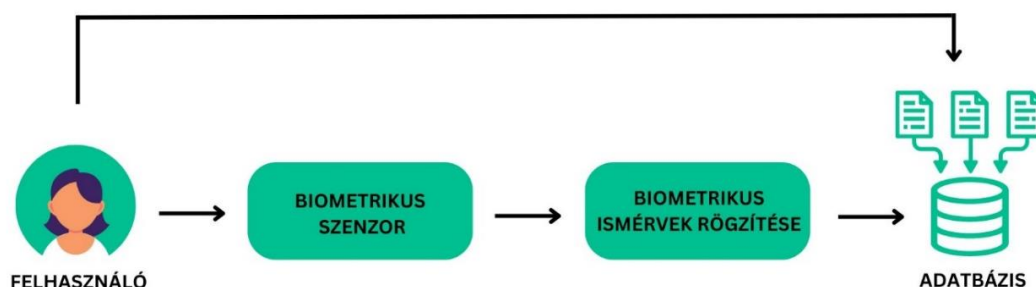
1. Fizikai jellemzők – például ujjlenyomat, tenyérlenyomat, arcfelismerés, a szemben található írisz mintázatának felismerése, DNS (dezoxiribonukleinsav), a szemben található retina felismerése (Liébana-Cabanillas et al., 2024), a fül vagy a kéz formája, vérerek mintázata (Mróz-Gorgoń et al., 2022)
2. Viselkedési jellemzők – például aláírás, billentyűleütés dinamikája, hangfelismerés (egyaránt fizikai és viselkedési jellemzőnek számíthat), kézírás, járásmód (Mróz-Gorgoń et al., 2022)
3. Kombinált jellemzők – azaz, fizikai és viselkedési jellemzők ötvöze, például beszéd felismerés (Sreekumar, 2010)

Egy személy hatékony felismerése érdekében a jellemzőknek változatlanak és egyedinek kell lenniük, viszont a biometrikus információk sem minden esetben nyújtanak 100%-os pontosságot. Az általánosan felhasznált biometrikus adatok a DNS (dezoxiribonukleinsav), az ujjlenyomat, a tenyérlenyomat, az arcfelismerés, a fül alakjának felismerése, a kéz- és ujjgeometria, a retina és az írisz felismerése, a járás, az aláírás és a hangfelismerés. Mára már világszerte elérhető ezen technológia, amely a felhasználók személyazonosságának ellenőrzésében és védelmében nyújt segítséget (Liébana-Cabanillas et al., 2024).

1.2.1 Az autentifikáció működési folyamata

A felhasználók autentifikációja egy adott rendszerbe, négy módon történhet: az egyén által ismert információk segítségével, mint például PIN kód vagy jelszó; a felhasználó által birtokolt tárgyak használatával, mint például chippel ellátott, okos kártyák. Továbbá „out-of-band” módon, amely eljárás során a bejelentkezés két különböző hálózattól kapott jelek alapján történik. Egy ismert példa ezen eljárásra, amikor egy személy bejelentkezik valamely fiókjába és egy ellenőrző számkódot vagy szöveget kap SMS formájában, amellyel e rendszer elfogadja a bejelentkezést (recfaces.com, 2021). Az utolsó mód pedig, maga a felhasználtól eredendő tulajdonságok segítségével, azaz biometrikus ismérvek alapján történő azonosítás. A hagyományos felhasználói bejelentkezés, az egyén tudására, valamint az általa birtokolt tárgyakra alapozódik, ebben az esetben az ügyfél jelszóval, PIN kóddal vagy okos tárgyakkal lép be egy adott rendszerbe. A biometrikus hitelesítési folyamat magába foglalja egy személy tulajdonságainak mérését, valamint összehasonlítását az adatbázisban levő ismérv másolatával. Ezen folyamat során fontos, hogy a rögzített biometrikus adatok kétségen kívül megegyezzenek az előzőleg tárolt mintával (Ogbanufe & Kim, 2018).

Azonosítás céljából a biometrikus rendszerek, két működési szakaszra vannak osztva, az első szakasz a regisztrációt feltételezi, míg a második szakasz az autentifikációt. A regisztráció esetében elsőként az egyén biometrikus adatai kerülnek megszerzésre. Ezen adatok hozzá vannak kapcsolva egy személyazonossághoz, majd végezetül kódokkal vannak ellátva és a rendszer adatbázisába vannak tárolva, abból a célból, hogy majd visszakereshetők és párosíthatók legyenek egy adott egyén ismérveivel (Clodfelter, 2010). Az adatok speciális szenzorokkal vannak beolvasva, majd ezen adatokból létrejön egy referenciasablon, amely egy adatbázisban vagy egy decentralizált eszközben, mint például mobiltelefon, kerül tárolásra (Clodfelter, 2010).



1 Ábra - Biometrikus regisztrációs (enrollment) folyamat

Forrás: Mróz-Gorgon et al., 2022, 4. o. alapján, saját szerkesztés

1.2.2 Identifikáció és verifikáció

Kontextustól függően, a biometrikus technológiát felhasználó rendszerek, két főle képpen működhetnek, identifikációs vagy ellenőrzési/verifikációs módban (Kumar & Ryu, 2009). Ameddig az identifikáció a „Ki ő a sok közül?” kérdésre ad választ, addig a verifikáció a „Ő X?” kérdésre válaszol, ahol X a feltételezett személyazonosság jelen esetben. Például akkor amikor egy személy bankkártya segítségével szeretne pénzt kivenni a bankautomatából, akkor a kártya segít az identifikációban. Mégpedig úgy, hogy a bankautomata leolvassa a kártyáról a számlaszámot, majd összehasonlítja az összes számlaszámmal, amely az adatbázisban található. Az egyén identifikációját követően, a felhasználó beírja a PIN kódját, amelyet a rendszer összehasonlít a számlaszámhoz rendelt PIN kóddal. Ez a folyamat jelenti a verifikációt/ellenőrzést. A biometrikus autentifikáció esetében is jellemzőek az előbbieken bemutatott identifikációs és verifikációs folyamatok (Sreekumar, 2010).

Az identifikáció esetében, a biometrikus ismérveket beolvasó eszköz, leolvassa az egyén biometrikus tulajdonságának mintáját, majd ezt összehasonlítja az adatbázisban tárolt összes többi mintával (Moriuchi, 2021), annak érdekében, hogy meghatározza az adott egyén személyazonosságát (Sreekumar, 2010). Ebben az esetben 1:N, azaz egy a sokhoz típusú megfeleltetés történik. Az “N” az adatbázisban levő minták számát jelképezi, ezen szám értékét figyelembe véve, a döntéshozatal (Match vagy No-Match, azaz megegyező vagy sem) folyamata hosszabb ideig is eltarthat. A beolvasott ismerv mintázatát, a rendszer az adatbázisban található, minden egyes mintával összehasonlítja, amíg egy megegyező mintát nem talál (Sreekumar, 2010). Az identifikáció során végbemenő folyamatot, a mellékletekben levő Ábra 1 (Identifikációs folyamat) szemlélteti.

Az ellenőrzési folyamat során, a rendszer az egyén személyazonosságát ellenőrzi és érvényesíti. Ebben az esetben az egyén állítja a személyazonosságát, például egy felhasználó név, egy dokumentum, egy bankkártya, egy okos kártya stb. segítségével. Ezt követően a rendszer összehasonlítja a beolvasott biometrikus ismérvet az adatbázisban levő, a felhasználónévhez, bankkártyához, dokumentumhoz stb. rendelt biometrikus tulajdonsággal (Kumar & Ryu, 2009). A verifikáció során 1:1, azaz egy az egyhez típusú megfeleltetés történik, amely esetében csak egyetlen, az adatbázisban levő mintát kell összehasonlítani a beolvasott ismerv mintájával, valamint csupán két alternatíva létezik a döntéshozatalt illetően, (Sreekumar, 2010), a hozzáférés elfogadott vagy elutasított (Clodfelter, 2010). Ezen ellenőrzési folyamat nagyrészt a mobiltelefonok feloldása, egy épületben való belépés, valamint a

bankszámlához való hozzáférés esetében használatos (Moriuchi, 2021). A verifikációs folyamatot szemléltető ábra a melléklete Ábra 2 (Verifikációs folyamat) mutatja be.

Az 1:N és az 1:1 megfeleltetések között megjelenik az 1:few, azaz egy a néhányhoz megfeleltetés, amely esetében a beolvasott biometrikus minta egy kisebb felhasználói csoport ismérveivel van összehasonlítva. Az adatbázisban már rögzített felhasználók száma nagyon változatos lehet, akár öt felhasználótól százakig mozoghat. Jelen esetben nincs egy pontos meghatározás arra, hogy mikor válik az 1:few megfeleltetés 1:N megfeleltetéssé (Sreekumar, 2010).

1.2.3 Adatvédelmi eljárások

Az Európai Unióra érvényes általános adatvédelmi rendeletben (GDPR) 9. cikkelye értelmében, a biometrikus adatok különösen érzékeny adatokként jelennek meg. Számos biometrikus autentifikációs folyamat létezik, amely elősegíti a biztonságot és az adatvédelemet. A biometrikus minták védelme érdekében számos módszer különböztethető meg, az első ilyen jellegű technológia a biometrikus kriptorendszer vagy az úgynevezett védett vázlatok, amelyek kriptográfia segítségével működnek. A második metódus, a biztonságos számítástechnikai eljárások használata, melynek célja két biometrikus minta összehasonlítása, annak érdekében, hogy beazonosítsa a nem megbízható felektől származó adatokat. A következő eljárás és egyben a legnépszerűbb metódus, a BioHashing algoritmus használata, amely “data salting” módszeren alapul (Liébana-Cabanillas et al., 2024). A “salting” algoritmus során, a jelszóhoz számos véletlenszerű karakter csatolódik, még mielőtt a “hashing” folyamat megkezdődne (Jung, 2021).

Az adavédelem érdekében a nyers biometrikus adatok feldolgozása minimális szinten kell történjen. Ehhez, az úgynevezett egyirányú adatfeldolgozás használata szükséges, amely egy kódot/sablont hoz létre a nyers biometrikus adatok mintájából. A létrehozott kód, az adatok lenyomatát jelképezi. Egy ilyen jellegű kód, továbbra is egyéni ismérvekkel rendelkezik, illetve összehasonlítható további kódokkal, így az ötlet a biometrikus adatok felhasználása mögött megmarad. Ezen megközelítés biztonságot nyújt a felhasználónak, akár a jelszóhash-ek (Mróz-Gorgón et al., 2022), amelyek során egy hash-elő algoritmus segítségével egy egyszerű szöveg betűk és számok nem értelmezhető sorozatává alakul (Jung, 2021). Ezen helyzetben az adatok biztonságban vannak, akkor is, ha a kód kiszivárog az adatbázisból, ugyanis az átalakított formája ezen kódnak már nem felhasználható (Mróz-Gorgón et al., 2022).

Az előbbieken felsoroltak mellett, a biztonság megőrzése és fokozása érdekében alkalmazható a törölhető biometria is (Manisha & Kumar, 2020). Ezen módszer során, egyetlen egyén biometrikus tulajdonságából, több azonosító kódot lehet létrehozni. Adott esetekben kitörölhető a már meglévő biometrikus azonosító minta és új sablont lehet létrehozni a nyers biometrikus adatból. Ezen biztonsági módszer, különösen hasznos, abban az esetben, ha megalapozott gyanúnk van arra, hogy valaki próbálja feltörni az adatbázist és próbálja felhasználni egy egyén azonosságát. Emellett abban az esetben is hasznos, amikor az adatbázisból kiszivárognak a biometrikus sablonokra vonatkozó adatok. Fontos, hogy a törölhető biometria használata esetében, a biometrikus adatok mellett, a rendszerbe más azonosítási források is szerepeljenek, mint például PIN kód vagy jelszó. Így megfelelő módon megváltoztatható a személyazonosság és könnyen összekapcsolható az újan generált sablonnal (Mróz-Gorgoń et al., 2022).

A biometrikus adatok védelmére szolgáló erőfeszítések, nem minden esetben bizonyulnak sikeresnek, egyes esetekben az ellenfeleknek sikerülhet az adatok birtokába jutni és felhasználni ezeket, azzal a céllal, hogy egy adott egyénnek vallja magát. Az ilyen jellegű hamisítások megelőzése érdekében felhasználható a liveness test, azaz életszerűség teszt (Mróz-Gorgoń et al., 2022). Ezen detektálás során, a rendszer feltételezi, hogy a bejelentkezett személy, nem valóban az igazi felhasználó, hanem egy bűnöző (Akhtar et al., 2015). Tulajdonképpen az életszerűség teszt felderíti, ha ténylegesen valódi biometrikus ismerv kerül a rendszerbe vagy biometrikus tulajdonságokat szimuláló tárgyak, valamint hamisított mintává megváltoztatott vagy ellopt biometrikus minták, mint például fényképek, videófelvevételek, maszkok stb. (Mróz-Gorgoń et al., 2022).

1.2.4 Biometrikus ismérveket felhasználó rendszerek működése

A biometrikus jellemzőket felhasználó rendszerek legelterjedtebb típusai közé sorolható az ujjlenyomat beolvasása, az arcfelismerés, az írisz felismerése, (Clodfelter, 2010), valamint a tenyérlenyomat. Legtöbb esetben a fiziológiai vagy fizikai ismérveket tekintik megfelelőbbnek, ezen rendszerek kialakítása során, mivel nem függnek az egyén adott pszichoemocionális állapotától (Babisch, 2012). A biometrikus ismérveket felhasználó rendszerek részletes leírása az 1 mellékletben olvasható.

1.3 A biometrikus technológia alkalmazása fizetési megoldásként

A biometrikus tulajdonságokat felhasználó technológiák különböző szakterületeken használatosak (Clodfelter, 2010), mint például igazságszolgáltatás, kriminalisztika - az

egyének felismerése érdekében, például áldozatok beazonosítása, egészségügy - páciensek beazonosítására (Ogbanufe & Kim, 2018), személyek azonosítása -például útlevél készítés során, biztonsági rendszerek esetében - például épületekbe való bejutás (Babisch, 2012), valamint kormányzati intézmények (Hwang et al., 2024), emellett a marketing területén is felhasználhatóak egyes biometrikus rendszerek, mint például a lojalitási kártyák használata esetében (Babisch, 2012). A kereskedelemben, valamint a banki és pénzügyi szektorokban is használatos (Ogbanufe & Kim, 2018).

Napjainkban a pénzügyi intézetek arra törekednek, hogy számos új technológiát vezessenek be, annak érdekében, hogy megkönnyítsék a fizetési folyamatot ügyfeleik számára. A fizetési rendszerek közül, a biometrikus fizetés a leginnovatívabb megoldást jelenti (Zarco et al., 2024). Ezen technológia, amely mesterséges intelligencia, big data, szenzorok és biometrikus adatokon alapul, jelentősen hozzájárul az ügyfélélmény javításához és a hatékonyság kiakasztásához (Hwang et al., 2024). A biometrikus technológia egyre nagyobb mértékű elfogadottságnak örvend a fogyasztók körében, az ujjlenyomat leolvasás mobiltelefonokba való integrálásának és a biometrikus rendszerek egyre inkább felhasználóbarátabbá tételének köszönhetően (Ogbanufe & Kim, 2018).

Zarco et al. (2024) meghatározása szerint a biometrikus fizetés egy olyan rendszert jelent, amely segít a tranzakciók hiteles végrehajtásában, felhasználva egy egyén saját biometrikus tulajdonságait. A fizetés végbemenésének engedélyezése, nem PIN kódok alapján történik, hanem az adott személy biometrikus azonosító ismérvei alapján, mint például az ujjlenyomat beolvasása, arcfelismerés, valamint hangfelismerés stb.

Ezen fizetési rendszernek legtöbb esetben két típusa van. Ez első típus a hibrid rendszer, amely esetében a biometrikus ismérveket ötvözve vannak a hagyományos fizetési módszerekkel, mint például egy chippel rendelkező bankkártyához, biometrikus adatokat rendelnek. A második típus, pedig olyan rendszereket feltételez, amelyek kizárólag biometrikus adatokat használnak fel egy tranzakció lebonyolításához (Zarco et al., 2024).

Az Európai Unió által megfogalmazott, elektronikus fizetési megoldásokat szabályozó pénzforgalmi irányelv (PSD2) szerint, megszüntetésre fognak kerülni azon fizetési módok, amelyek kizárólag a kártya adatokkal történnek. Ezen irányelv a vállalkozások és pénzügyi intézményektől megkövetel legalább egy megoldást a következő hitelesítési technológiák közül: valami, amit csak a felhasználó tud (PIN kód), valami, amit a felhasználó megismer (üzenetben kapott kód), valami, ami a felhasználótól eredendő (biometrikus jellemzők). Ezen irányelv bevezetése a biometrikus fizetési lehetőségek implementálást is nagymértékben megnövelte (Liébana-Cabanillas et al., 2024).

1.3.1 Biometrikus fizetési megoldások működése

Biometrikus bankkártya

A biometrikus bankkártya használata képezi az egyik biometrikus fizetési modalitást, amely során a chiptechnológiát párosítják az ügyfél ujjlenyomatának mintázatával, annak érdekében, hogy a kártyatulajdonos személyazonosságát biztonságosan és kényelmesen ellenőrizni lehessen (Zarco et al., 2024). Ezen fizetési megoldás során, a kártyatulajdonos biometrikus adatainak rögzítése és tárolása a kártyán történik, így ezen adatok “nem hagyják el” a bankkártyát. Egy tranzakció során, a kártyába épített szenzor érzékeli az ügyfél ujjlenyomatát és összehasonlítja a kártyában bekódolt ujjlenyomat sablonnal. Így a kártya birtokosának nem szükséges PIN kódot megadnia. Abban az esetben, ha az azonosítás hiteles volt, végbe is megy a tranzakció (mastercard.us, 2023).

Biometrikus regisztráció alapú alkalmazások, rendszerek

Egy további biometrikus fizetési technológia, a felhasználók olyan rendszerekbe való regisztrálását feltételezi, amelyeknek részesei adott kereskedelmi egységek, ahol van lehetőség biometrikus ismérvek segítségével fizetni (Kumar et al., 2008). Ebben az esetben, a biometrikus fizetést megelőzően, a felhasználó regisztrál az adott rendszerbe, alkalmazásba, telefonon keresztül, ahol egy elektronikus pénztárcát hoz létre, majd beolvassa az adott biometrikus ismérvet, mint például az ujjlenyomatot vagy az arc képet, majd hozzárendeli azon bankkártya adatokat, amelyekről a továbbiakban a fizetés fog történni (Clodfelter, 2010). Ezen folyamat gyors, csupán két percet igényel. A fizetés mellett ezen alkalmazások, sok esetben biztosítanak hűségprogramokban való részvételt, ajándékutalványokat, valamint kedvezményes kuponokat is (Kumar et al., 2008). A regisztrációt követően, a fizetés során nem szükséges a bankkártya használata. A fogyasztó egyszerűen a rögzített biometrikus ismérvvel fizet, az ehhez kihelyezett szenzorok segítségével, mint például az ujjlenyomat odaérintése ezen szenzorhoz (Clodfelter, 2010).

Ezen alkalmazások lehetnek általánosan használhatóak, több kereskedelmi egység esetében, vagy korlátozva vannak egy adott kereskedelmi egységre vagy egység csoportra (visa.navigate.com, 2022). Ilyen rendszerek közé tartozik például a Kínában használt Alipay – Smile-to-pay, WeChatPay – FrogPro (theguardian.com, 2019), egyes bankok mobilapplikációi, PopID alkalmazás (visa.navigate.com, 2022), Well.com felület (Imbrea, 2018), PayEye (payeye.com) stb.

Emellett, egy másik regisztrációt feltételező biometrikus fizetés is megemlíthető. Hasonlóan az előző modalitásokhoz, a felhasználó beolvassa a biometrikus ismérvet az

alkalmazáson keresztül. Ezt követően bevezeti adatait, jelen esetben szükséges egy azonosító adat, rendszertől függően, egy PIN kód, jelszó vagy a személy telefonszáma, amely a biometrikus ismértvhez van rendelve. A regisztrációt követően a fizetés során beolvasásra kerül, például az ujjlenyomat, illetve a vásárlónak be kell írnia a telefonszámot vagy a PIN kódot a tranzakció végbemenetele érdekében (Kumar et al., 2008).

Az alkalmazásokon keresztül történő regisztráció mellett, megemlíthető a kereskedelmi egységekben történő bejelentkezés is, amely során a felhasználó egy adott biometrikus tulajdonsága beszkennelésre kerül az adott kereskedelmi egységbe található speciális szenzor segítségével. Ezt követően a felhasználó beírja telefonszámát, valamint a fizetési adatait, például kártyaszám, a rendszerhez több kártya is hozzáadható. A fiók létrehozása után, a biometrikus ismértv megjelenik az adatbázisban, majd a vásárló a pénztárnál levő leolvasóhoz érinti például az ujjlenyomatát, majd beírja telefonszámát, végezetül pedig kiválasztja azon bankkártyát amivel fizetni szeretne (Kumar et al., 2008).

Ezen fizetési megoldások előnyei és hátrányai bemutatásra kerülnek a 2. mellékletben.

1.4 Innovatív fizetési megoldások használati szándékának kutatásai

Liébana-Cabanillas et al. (2024) által végzett kutatás célja, megvizsgálni a technológia elfogadásának és használatának egységes elmélet 2 (UTAUT2) elemeinek hatását, valamint az észlelt kockázat hatását a biometrikus mobilfizetési rendszerek használati szándékára. Ezen kutatás Spanyolországban került elvégzésre. A kutatási módszertant illetően, elsőként egy kvalitatív, szakértői mélyinterjú került elvégzésre. Ezen kutatás segítségével szolgált, az ezt követő kvantitatív, kérdőíves kutatáshoz szükséges kérdések és skálák átfogalmazásában. Az online kérdőíves kutatás 2020 november és 2021 január között zajlott. A kutatás a PayEye biometrikus fizetési alkalmazásra fókuszált. A minta 2586 okostelefon felhasználóból állt. A téma jobb megértése érdekében, a kérdőív kitöltése előtt, egy videó keretén belül bemutatásra került a PayEye biometrikus fizetési megoldás.

A kutatás eredményeit tekintve, a használati szándékot befolyásoló legjelentősebb változók az elvárt teljesítmény, az észlelt erőfeszítés, a hedonikus motiváció, valamint a kockázat észlelés volt. Ezzel szemben, a szubjektív normák, az árérték arány, valamint a megszokott magatartás gyengébb hatással volt, a használati szándékra.

Egy 2023-ban, Spanyolországban végzett kutatás során, megvizsgálásra került a biometrikus fizetés, két egymást kiegészítő kutatás segítségével. Az első kutatás, egy kvantitatív, online kérdőíves kutatás volt, amely célja a biometrikus fizetési technológia

használatának előrejelző változóit meghatározni. Ezen kutatáshoz, egy integrált modell volt felhasználva, amely a technológia elfogadásának és használatának egységes elmélet 2 (UTAUT2), az általános kockázat elmélet (General Risk Theory) és a bizalom elmélet (Trust Theory) tette ki. A vizsgált mintaszám 1905 volt. A második kutatást, egy kvalitatív kutatás tette ki. Ennek során két csoportra osztva, 10-10 fintech iparági szakértővel készültek mélyinterjúk, annak érdekében, hogy elemzésre és összehasonlításra kerüljenek a kérdőívben kapott eredmények (Zarco et al., 2024).

A két kutatási módszert követően, a kapott eredmények, arra mutatnak rá, hogy az észlelt kockázat, a bizalom, valamint a szubjektív normák azok a változók, amelyek a szakértők tapasztalata szerint a legfontosabbak a felhasználók számára, a biometrikus fizetési módszerek használatát tekintve (Zarco et al., 2024).

Egy további kutatás, 2013-ban, Kínában lett elvégezve, ezen tanulmány célja, megvizsgálni, hogy különböző bizonytalansági tényezők, hogyan akadályozzák a mobilfizetés elfogadását. A kutatás során felhasznált modell a bizonytalansági-kockázat-érték (uncertainty-risk-value framework) keretrendszer, amely az észlelt kockázat elmélet (Perceived Risk Theory), a kilátáselméleten (Prospect Theory) és az észlelt érték elméleten (Perceived Value Theory) alapul. A kutatómódszertant tekintve, kvantitatív, online kérdőíves megkérdezés volt, amely során 310 kitöltésre került sor (Yang et al., 2015).

Az eredményeket illetően, a felhasználók által észlelt pénzügyi kockázat jelentősen negatív hatással van az észlelt értékre. Emellett az észlelt pénzügyi kockázat a legjelentősebb negatív tényező, amely akadályozza a mobilfizetés elfogadását a fogyasztók által. Továbbá az észlelt információs aszimmetria, az észlelt technológiai bizonytalanság, az észlelt szabályozási bizonytalanság és a szolgáltatás érzékelt megfoghatatlansága, fő meghatározó tényezők az észlelt kockázat esetében. Ezenfelül, az észlelt teljesítménykockázat és az észlelt adatvédelmi kockázat erős negatív hatást gyakoroltak az észlelt értékre és az elfogadási szándéokra (Yang et al., 2015).

Reepu & Arora (2022) Indiában végzett, kutatásának célja, megvizsgálni az észlelt kockázat hatását az online bankhasználatra. Ezen kutatás kategorizálva, felmérte a különböző észlelt kockázatok hatását az online banki ügyintézésre, a megvizsgált kockázatok közé sorolható, az adatvédelem, a társadalmi kockázat stb. A kutatás elvégzése érdekében, kvantitatív, kérdőíves kutatást alkalmaztak, a minta 226 női válaszadóból tevődött össze.

A kutatás eredményei azt mutatták, hogy az adatvédelmi kockázat és a biztonsági kockázat változók vannak a legnagyobb hatással, ezt követi a társadalmi kockázat időbeli

kockázat és a pénzügyi-teljesítmény kockázat, amelyek negatív hatással vannak az online banki ügyintézés használati szándékára.

A fent említett kutatások eredményeinek összefoglalása, a mellékletekben található Táblázat 2 (Áttekintett kutatások összefoglalása) mutatja be.

2. Konceptuális modell és hipotézisek

A tudományos szakirodalom számos viselkedési döntéselméletet, illetve szándékot meghatározó modellt dolgozott ki, annak érdekében, hogy megvizsgálja az egyének különféle innovációkra adott válaszait. Ezen elméletek és modellek számos esetben szociálpszichológiai kutatásokon alapulnak (Zarco et al., 2024).

A különböző információ technológiai és marketing kutatások, számos modellt és elméletet hoztak létre a fogyasztók internetes magatartását vizsgálva (Zarco et al., 2024). Zarco et al., (2024) kiemeli ezen területen széleskörben használt elméleteit: a megalapozott cselekvési elmélet (TRA) (Fishbein & Ajzen, 1975), a technológiaelfogadási modell (TAM) (Davis et al., 1989), valamint a tervezett viselkedés elmélete (TPB) (Ajzen, 1991).

Emellett, Venkatesh et al. (2003) javasolta a technológia elfogadásának és használatának egységes elméletét (UTAUT). A továbbiakban, a technológia folyamatos fejlődésének köszönhetően a fogyasztók körében, szükséges volt, ezen elmélet kiterjesztésére, hangsúlyt téve a hedonikus értékekre is egyaránt. Így az elmélet kibővült, három új változóval, a hedonikus motiváció, az árérték arány, valamint a megszokott viselkedés. A változók kibővítése során, létrejött a ma közismert technológia elfogadásának és használatának egységes elmélete 2 (UTAUT2). A tudományos szakirodalomban, ezen modell, az egyik legszélesebb körben használt, a technológiai innovációk elfogadásának megvizsgálása esetében (Tamilmani et al., 2021).

Liébana-Cabanillas et al., (2024), valamint Zarco et al. (2024) biometrikus fizetési módszerek elfogadásának kutatása során, ezen elmélet került felhasználásra, mivel egy mélyebb megértést nyújt, a viselkedési szándékot befolyásoló tényezők megvizsgálásában.

Emellett, ezen modellt, egyéb kutatások, kifejezetten az innovatív fizetési megoldások során, például a mobilfizetés, használati szándékának megvizsgálására használták (Liébana-Cabanillas et al., 2024).

Az alábbiakban bemutatásra kerül a UTAUT 2 modell, várható teljesítmény (performance expectancy), várható erőfeszítés (effort expectancy), szubjektív normák (subjective norms), elősegítő feltételek (facilitating conditions), hedonikus motiváció (hedonic motivation), illetve megszokott viselkedés (habit) változói. Jelen kutatásban az ár-

érték arány változó nem került a konceptuális modellbe, mivel általánosságban kerülnek megvizsgálásra a biometrikus fizetési megoldások, ezen technológiák többsége ingyenesen elérhető. Ezt követően bemutatásra kerül az első kutatási kérdés, valamint a hipotézisek megfogalmazása, az előbbiekben említett változók alapján.

K1: Melyek azok a tényezők, amelyek hatnak a fogyasztók biometrikus fizetési megoldások elfogadására és használati szándékára?

A várható teljesítmény arra vonatkozik, hogy egy egyén mennyire hiszi abban, hogy egy adott technológiának a használata elősegíteni, javítani fogja teljesítményét (Venkatesh et al., 2003). Liébana-Cabanillas et al., (2024) kutatása szerint, a várható teljesítmény az egyik legjelentősebb befolyásoló tényező, amely elősegíti a biometrikus mobilfizetési megoldások használati szándékát. A biometrikus mobilfizetési technológiát felhasználók jellemzően kihasználják ezen technológia által nyújtott előnyöket, amelyek egy magasabb felhasználási arányhoz vezetnek (Liébana-Cabanillas et al., 2024). Így a várható teljesítményre vonatkozóan, a következő hipotézis került megfogalmazásra:

H1: A várható teljesítmény pozitív hatással van a biometrikus fizetési megoldások használati szándékára.

Várható erőfeszítés

A várható erőfeszítés a fogyasztók által érzékelt egyszerűség mértékére vonatkozik, egy technológia felhasználása esetében (Venkatesh et al., 2012). Annak függvényében, hogy egy egyén milyen mértékben gondolja egyszerűnek vagy nehéznek a biometrikus fizetési megoldások használatát, többé vagy kevésbé hajlandó igénybe venni azon technológiát (Liébana-Cabanillas et al., 2024). A várható erőfeszítés, egy jelentős befolyásoló tényező a biometrikus rendszerek fizetési folyamatok, valamint a pénztárnál való használat során (Ogbanufe & Kim, 2018). Ezen esetben a következő hipotézis fogalmazható meg:

H2: A várható erőfeszítés pozitív hatással van a biometrikus fizetési megoldások használati szándékára.

Szubjektív normák

A szubjektív normák változó arra vonatkozik, hogy mások (például fontos személyek, közeli ismerősök, családtagok, barátok stb.) véleménye milyen mértékben befolyásolja az egyén, egy adott technológia használatát (Venkatesh et al., 2012). Zarco et al. (2024) szerint, a szubjektív normák erős hatást gyakorolnak abban, hogy egy személy milyen mértékben használja a biometrikus kártya fizetési megoldást. Egy új, innovatív biometrikus fizetési módszer esetében, megtörténhet, hogy az egyének számára ezen technológia ismeretlen, bizonytalannak érezhetik magukat. Így, az általuk fontosnak, megbízhatónak talált személyek véleményére hallgatnak (Liébana-Cabanillas et al., 2024). A következő hipotézis merül fel:

H3: A szubjektív normák pozitív hatással vannak a biometrikus fizetési megoldások használati szándékára.

Elősegítő feltételek

Az elősegítő feltételek, arra vonatkoznak, hogy egy egyén milyen mértékben rendelkezik az adott technológia használatához szükséges erőforrásokkal, valamint milyen mértékben kap segítséget más személyektől, abban az esetben, ha nehézségeket érzékel az új technológiai használata során (Venkatesh et al., 2012). A biometrikus mobilfizetési technológia, új, még nem széleskörben elterjedt a használata, így az egyéneknek szükségük lesz különböző készségekre, annak érdekében, hogy felhasználják ezen rendszereket. Abban az esetben, ha a felhasználók rendelkeznek az adott ismeretekkel, illetve erőforrásokkal, jellemzőbben használni fogják az új technológiát (Liébana-Cabanillas et al., 2024). A következő hipotézis kerül megfogalmazásra:

H4: Az elősegítő feltételek pozitív hatással vannak a biometrikus fizetési megoldások használati szándékára.

Hedonikus motiváció

A hedonikus motiváció, egy technológia használata során észlelt élményből származó élvezet vagy szórakozás érzete. Ezen motiváció fontos szerepet játszik egy adott technológia elfogadásában és használati szándékában (Venkatesh et al., 2012). Liébana-Cabanillas et al., (2024) kutatásában a hedonikus motiváció elemzésének fő célja az egyének érzelmeinek és reakcióinak megvizsgálása a biometrikus mobilfizetési rendszerre vonatkozóan. A kutatás során, a hedonikus motiváció az egyik legerősebb hatást gyakorolta a biometrikus mobilfizetési

technológia használati szándékára. Ezen motiváció mögötti racionalitás feltételezi, hogy minél inkább élvezetesebb, szórakoztatóbb egy technológia használata, annál inkább hajlandóak lesznek az egyének elfogadni és igénybevenni. Ezen tény annak köszönhető, hogy az egyénekre jellemző, hogy olyan irányban cselekedjenek, amely minél inkább pozitív élményeket nyújt számukra (Liébana-Cabanillas et al., 2024). A következő hipotézis fogalmazható meg:

H5: A hedonikus motiváció pozitív hatással van a biometrikus fizetési megoldások használati szándékára.

Megszokott viselkedés

A megszokott viselkedés vagy szokás, arra vonatkozik, hogy az egyének hajlamosak különböző viselkedéseket automatikusan elvégezni, annak köszönhetően, hogy ezen viselkedések már megtanulásra kerültek. A megszokott viselkedés, két kategóriába sorolható, elsőként, a megszokott viselkedés, korábbi viselkedésként van tekintve. Másrészt pedig, a szokás, abban mutatkozik meg, hogy az egyén milyen mértékben gondolja azt, hogy egy adott viselkedés automatikussá válhat saját esetében (Venkatesh et al., 2012). Liébana-Cabanillas et al. (2024) kutatása során a megszokott viselkedést úgy határozza meg, mint az a mérték, amelyben egy egyén automatikusan végrehajt egy bizonyos viselkedési formát, a megszerzett tudás következtében. Ezen tény növeli a biometrikus mobilfizetési módszerek használati szándékát (Liébana-Cabanillas et al., 2024). A következő hipotézis kerül megfogalmazásra:

H6: A megszokott viselkedés pozitív hatással van a biometrikus fizetési megoldások használati szándékára.

Továbbá, Az UTAUT 2 modell kiegészítésre kerül, az észlelt kockázat elmélettel (Perceived Risk Theory), a biometrikus fizetési megoldások elfogadásának és használati szándékának kontextusában (Liébana-Cabanillas et al., 2024; Zarco et. al 2024). Az észlelt kockázat elmélet felhasználásra került, mivel a mobilfizetés elfogadásának is, egyik legfontosabb változójaként van említve (Liébana-Cabanillas et al.,2024).

Bauer (1960) nevéhez fűződik, az észlelt kockázat elmélet, amely az ügyfelek viselkedésének magyarázatára volt használatos. Az észlelt kockázat ezen esetben egy veszteségérzetet jelképez (Reepu&Arora, 2022). Ezen tanulmány értelmében, bizonyos kockázatok jelennek meg, a fogyasztók vásárlási magtartásában, mivel a vásárlási döntéseknek

kiszámíthatatlan vagy kedvezőtlen eredményei lehetnek (Liébana-Cabanillas et al., 2024). Az észlelt kockázat ötdimenziós modellje, főként a mobilfizetés esetében használatos és a további kockázatokra feltételezi: észlelt pénzügyi kockázat, adatvédelmi kockázat, teljesítményre vonatkozó kockázat, pszichológiai kockázat, valamint időbeli kockázat (Yang et al., 2015).

Jelen kutatás során ezen elmélet, két változói kerülnek megvizsgálásra, az észlelt adatvédelmi, valamint az észlelt pénzügyi kockázat változók, mivel különböző innovatív fizetési megoldások elfogadását elemző kutatások, mint például mobil fizetés, valamint online banki ügyintézés során, a legerősebb hatást fejtették ki az elfogadási, valamint a használati szándékra (Reepu&Arora, 2022; Yang et al., 2015). A következő kutatási kérdés került megfogalmazásra:

K2: Melyek azok a kockázati tényezők, amelyek negatív hatással vannak a fogyasztók biometrikus fizetési megoldások elfogadására és használati szándékára?

Észlelt pénzügyi kockázat

Bár a biometrikus technológia általánosan véve biztonságosabb és nehezebben feltörhető, vannak esetek amikor viszont felmerülhet ezen veszély (Liébana-Cabanillas et al., 2024). Az észlelt pénzügyi kockázat a fogyasztók lehetséges pénzügyi veszteségének észlelésére vonatkozik, különféle okok miatt, mint például a mobilfizetés esetében a jelszavak feltörése, ennek következtében, nem kívánt személy is hozzáférhetnek egy egyén pénzügyeihez (Yang et al., 2015). Yang et al. (2015) kutatásának eredményei során, a pénzügyi kockázat fejtette ki a legnagyobb negatív hatást a mobilfizetés használati szándékára. A következő hipotézis kerül megfogalmazásra:

H7: Az észlelt pénzügyi kockázat negatív hatással van a biometrikus fizetési megoldások használati szándékára.

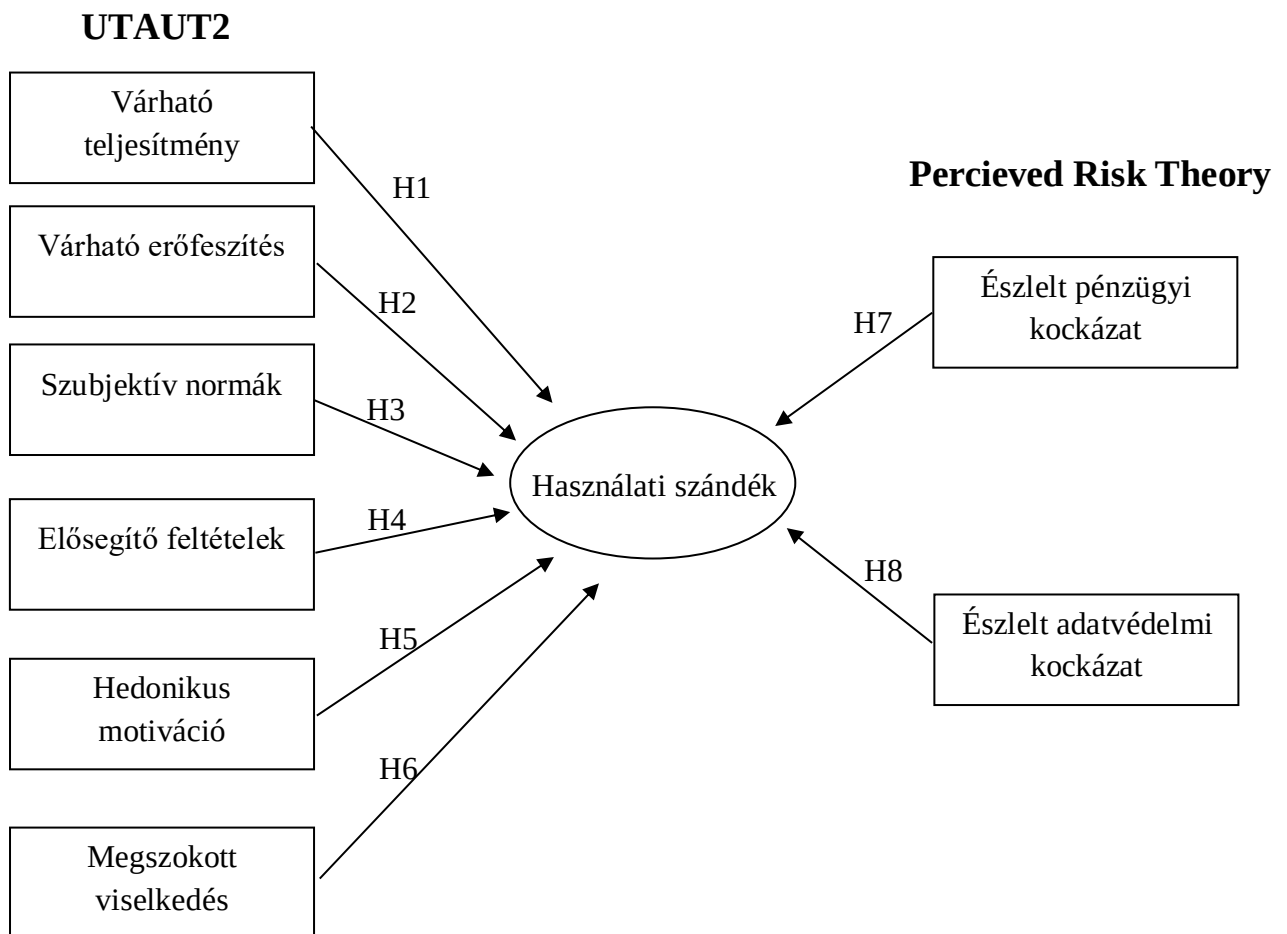
Észlelt adatvédelmi kockázat

A biometrikus adatok, érzékeny adatoknak vannak tekintve, így több szinten is szükség van ezen adatok védelmére (Mróz-Gorgoń et al., 2022). Az adatvédelem egy fő szempont a mobilfizetési megoldások esetében, mivel számos személyes információ felhasználásra kerül ezen technológia igénybevétele során. A felhasználók által észlelt kockázatok közé tartozik a személyes információk kiszivárgása és nem kívánt célokból való felhasználása, más személyek által (Yang et al., 2015). Reepu&Arora (2022) kutatása során az észlelt adatvédelmi kockázat

volt a legnegatívabb hatással az online bank ügyintézési használati szándékra. A következő hipotézis fogalmazható meg:

H8: Az észlelt adatvédelmi kockázat negatív hatással van a biometrikus fizetési megoldások használati szándékára.

Az alábbi ábra bemutatja a kutatásom során használt konceptuális modellt, illetve a modellben vizsgálendő változókat és hipotéziseket. Ezen elemek, a további fejezetben kerülnek elemzésre kérdőíves kutatás segítségével.



2 Ábra - Konceptuális modell és hipotézisek

3. Alkalmazott kutatási módszertan

Az előző fejezetekben bemutatásra került a témának megfelelő és releváns szakirodalom, azon kutatások eredményei, amelyek egy alapot biztosítanak jelen kutatás elvégzéséhez, valamint a piaci helyzet. Ezen fejezet során a primer kutatást tárgyalom, bemutatva a választott kutatási módszert, annak előnyeit és hátrányait, valamint a kutatás

részleteit. Ezt követően, bemutatásra kerül a kutatás során használt kérdőív, a mintavétel, valamint az adatgyűjtés folyamata.

3.1 A kutatási módszertan bemutatása, előnyei és hátrányai

Jelen kutatás célja, megvizsgálni a biometrikus fizetési megoldások elfogadását és használati szándékát befolyásoló tényezőket, a romániai fogyasztók körében. A felvetett kutatási kérdések, valamint a szakirodalom alapján megfogalmazott hipotézisek tesztelése érdekében kérdőíves kutatást végeztem.

A kvantitatív kutatás célja, a kapott adatok számszerűsítése, statisztikai elemzéseket végezve, illetve általánosítások megfogalmazása az elemzett populációra, a minta alapján. Ezen kutatási módszer jól strukturált adattgyűjtést feltételez. Az egyik legelterjedtebb formája, a kérdőíves megkérdezés, amely egy strukturált adatgyűjtési módszer, amely esetében a sokaság egy mintája válaszol, azzal a céllal, hogy a megkérdezettektől adott információk kerüljenek begyűjtésre. A kérdőívben található kérdések különböző témákra kérdezhetnek rá, mint például a válaszadók attitűdje, ismereteik, magatartásuk, szándékaik és motivációik (Malhotra & Simon, 2017).

Jelen kutatásban felvetett kutatási kérdések megválaszolása érdekében, a kérdőíves kutatás bizonyult a legmegfelelőbb módszernek. Elsőként, a kutatás fő célja a fogyasztók használati szándékának, illetve technológia elfogadásának vizsgálata, így szükséges egy nagyobb mintán alapuló megkérdezés ahhoz, hogy mintázatok és összefüggéseket azonosítsunk be. Az adatgyűjtés strukturált jellegéből adódóan, a szakirodalomban áttekintett kutatásokban szereplő modellek változói, előre megtervezett felépítés alapján kerülhettek megválaszolásra, valamint az összes válaszadó ugyanazon kérdésekre adott választ, egy adott sorrendet követően. A kérdőívben egyetlen egy nyílt kérdés szerepelt, így a nagyrésze zárt kérdésekből tevődött össze, amelyek lehetővé teszik, a megkérdezettek válaszainak számszerűsítését, majd ezt követően a statisztikai elemzését (Malhotra & Simon, 2017).

Továbbá a kérdőíves kutatás bizonyult a legalkalmasabb és leggyakrabban használt megoldásnak a szakirodalomban, a biometrikus fizetési megoldások, valamint az innovatív fizetési megoldások használati szándékának és elfogadásának felmérésére.

A kérdőíves megkérdezés számos előnnyel rendelkezik, viszont különböző hátrányok is felmerülhetnek ezen kutatási módszer alkalmazása tekintetében.

Előnyök

Az előnyöket tekintve, az egyik legnagyobb előnye ezen adatgyűjtési módszernek, a nagymennyiségű adat összegyűjtése, viszonylag kevés idő alatt. A kutatásomban online

kérdőíves megkérdezést használtam, így több személyhez is eljuthatott a kérdőív, nagy mintát lehetett elérni ezen módszerrel. A válaszadók nem szembesültek időbeli, valamint térbeli korlátokkal, a kérdőívet bármikor, bárhol kitölthették, valamint a válaszok teljes mértékben anonimak, így a hitelesebbnek tekinthetők, mivel nem lépett fel, társadalmi elvárás, befolyás. Egy további előny, amely a kérdőíves kutatásból származik, a kérdések strukturájának köszönhetően, a begyűjtött adatok, egyszerűen számszerűsíthetők és statisztikailag elemezhetők (Malhotra & Simon, 2017).

Hátrányok

A kérdőíves kutatás hátrányait illetően, az egyik hátrányt képezi az, hogy a kitöltők nem minden esetben képesek alkalmas információkat megadni. Továbbá a kérdőív rögzített strukturája miatt, nem kerülnek megismerésre további esetleges háttérinformációk, kizárólag a feltett kérdésekre érkezik válasz (Malhotra & Simon, 2017).

Az online kérdőíves megkérdezés során egy hátrányt jelenthet, hogy a válaszadó félre értelmezi, nem helyesen értelmezi a feltett kérdéseket, mivel saját maga tölti ki, nem kap segítséget a kérdezőbiztostól. Ezen okból kifolyólag, nem a megfelelő válaszok érkezhetnek (Malhotra & Simon, 2017).

3.2 A kérdőív felépítése és mérés

A kutatásom során használt kérdőív 4 részre osztható. Az első részben megtalálható a leírás, amelyben a válaszadó értesül a kutatás céljáról és feltételeiről, valamint a biometrikus fizetési megoldások meghatározása is megjelenik, egy rövid magyarázatként, a kutatás témájának jobb megértése érdekében. Ezt követően 3 feleletválasztós, bevezető kérdés volt, amely a válaszadók mindennapi fizetési szokásaikra kérdez rá, milyen mértékben használnak készpénzzel, bankkártyával való fizetést, valamint mobilfizetést (például BTPay, ApplePay, GooglePay, stb.).

A bevezető kérdéseket követően, egy alternatív zárt kérdés volt, amely szűrőkérdésként jelent meg. A válaszadónak kikellett jelölnie, ha használt-e már valaha biometrikus fizetési megoldásokat vagy sem.

Abban az esetben ha a szűrőkérdésre a válasz „nem” volt, a kérdőív összesen 41 kérdést tartalmazott. Az első szakaszt követően, a kérdőív folytatódott a következő szakasz kérdéseivel, amelyek a felhasznált konceptuális modell elemienek vizsgálatára szolgáltak. Mindenik elem esetében egy 1-től 5-ig (1- egyáltalán nem értek egyet, 5- teljes mértékben egyet értek) terjedő Likert skála került használatra, az állítások mérése érdekében. A legtöbb változó 3 elemet tartalmazott (várható teljesítmény, elősegítő feltételek, hedonikus motiváció,

megszokott viselkedés, észlelt pénzügyi kockázat, észlelt adavédelmi kockázat, használati szándék), valamint 2 változó, 4 elemet (várható erőfeszítés változó, szubjektív normák). Az állítások az összes változó esetében a szakirodalom alapján lettek megfogalmazva. Két változó kivételével (észlelt pénzügyi kockázat, észlelt adavédelmi kockázat), az összes változó (Liébana-Cabanillas et al. (2024) által használt skálák alapján lettek megfogalmazva. Ez előbbieken említett kutatásokok során, a skálák Venkatesh et al. (2003), illetve a Venkatesh et al. (2012) által javasolt UTAUT2 modell alapján kerültek adaptálásra a biometrikus fizetési megoldások kontextusára. Kutatásomban, UTAUT2 modell ár-érték arány változója nem került felmérésre, mivel általánosságban kerülnek megvizsgálásra a biometrikus fizetési megoldások, ezen technológiák többsége ingyenesen elérhető. Az észlelt pénzügyi kockázat és adavédelmi kockázat állításai, pedig Yang et al., (2015) alapján lettek megfogalmazva.

Abban az esetben, ha a válasz „igen” volt, egy további feleletválasztós kérdés jelent meg. Ezen kérdés rákérdezett arra, hogy a válaszadó milyen biometrikus fizetési megoldásokat használt, ebben az esetben, több válaszlehetőség volt bejelölhető (ujjlenyomat, tenyérlenyomat, arcfelismerés, írisz mintázatának felismerése, hangfelismerés), valamint az egyéb résznél, a válaszadó beírhatott egy további, általa használt biometrikus fizetési megoldást is. A szűrőkérdésre igennel válaszolók esetében a kérdőív összesen 42 kérdésből tevődött össze. Ezen kérdést követően, az előbbieken említett és részletezett „nem” válaszhoz hasonlóan, a konceptuális modell elemeinek használt állításai következtek.

Az két választási lehetőség, „nem”, valamint „igen” állításai között a különbséget az állítások megfogalmazása adta. Az „igen” válaszok során, állító mondatok lettek megfogalmazva, valamint a „nem” válaszok során az állítások feltételes módban lettek megfogalmazva.

A kérdőív 3. szakaszában egy nyílt kérdés volt, amely esetében a válaszadó röviden összefoglalhatta véleményét a biometrikus fizetési megoldásokról.

Az utolsó szakaszt pedig a demográfiai kérdést tették ki: nem, életkor, állandó lakhely típusa, megye, legmagasabb iskolai végzettség, jelenlegi foglalkozás, valamint havi jövedelem.

A kérdőív szerkezetének bemutatása, a mellékletekben található Táblázat 3 (A kérdőív szerkezete) ábrázolja.

3.3 Mintavétel és adatgyűjtési folyamat

A kutatás célsokaságát a Romániában élő, román és magyar, 18 éven felüli fogyasztók képezik. A mintavételi eljárás nem véletlenszerű volt, valamint a fogyasztók alacsony kitöltési hajlandósága miatt, alacsony számú kitöltés lett, így a minta nem tekinthető reprezentatívnak.

A kérdőív a Facebook közösségi média oldalon került megosztásra, majd Instagram Story segítségével is eljutott további személyekhez. Elsőként az ismerőseim körében lett megosztva, majd a hóladba módszert alkalmazva, arra voltak kérve, hogy továbbítsák a kérdőívet ismerőseiknek. Az ismerősi kör mellett, 2 magyar Facebook csoport, illetve 3 román Facebook csoportban került megosztásra a kérdőív. Ennek célja, az volt, hogy minél több személy kitöltse, viszont ezen Facebook csoportok tagjainak, jelentős része egyetemi hallgató voltak, így a minta ezen okból sem tekinthető reprezentatívnak.

A kérdőív elsőként magyar nyelven lett megszerkesztve, majd ezt követően lefordítottam román nyelvre is, annak érdekében, hogy több fogyasztót elérjen. Az online kérdőív a Google Forms kérdőív szerkesztő platform felhasználásával lett összeállítva, majd ugyanezen platform segítségével, k begyűjtésre kerültek a válaszok. A kérdőív publikussá tétele előtt, tesztelésre került, annak érdekében, hogy a kérdések minél egyértelműbbek legyen a további válaszadók számára. A tesztelés során 5 román és 7 magyar személy töltötte ki a kérdőívet. Az eredeti változat leírásában szerepelt egy videó, amely magyarázatot adott a biometrikus fizetési megoldásokat illetően. A tesztelés során viszont, kiderült, hogy azon videó, nem bizonyult hasznosnak. A videóba az Amazon One biometrikus fizetési megoldás kerül bemutatásra, viszont kutatásom általánosságban vonatkozik a biometrikus fizetési megoldásokra, így inkább összezavarta a tesztelés során a kitöltőket. Emellett a videó megtekintése időigényesnek bizonyult, így a végső változat leírásában a biometrikus fizetési megoldások meghatározása került be magyarázatként.

Az adatgyűjtés 2024 április 24 és 29 között zajlott és összesen 185 kitöltés érkezett, amelyből 83 kitöltés a kérdőív magyar változatára, valamint 102 a román nyelvű változatra.

Az adatok tisztítása során 9 választ került eltávolításra, mivel 5 válasz során a nyílt kérdésre megírt válasz alapján kiderült, hogy a válaszadó félreértelmezte a kutatás témáját. Emellett 6 válasz kizárásra került, mivel minden állítás esetében ugyanazon válaszok lettek megadva. Ezt követően 176 válasz maradt. A szűrőkérdés alapján, az adattisztítást követően 148 válaszadó nem használt biometrikus fizetési megoldásokat, valamint 28 válaszadó használt. Az „igennel” válaszolókat mintaszáma nagyon alacsonynak bizonyosult, így nem készülhett volna egy különálló statisztikai elemzés. Így a végső mintaszám 148 volt, amelyet azon fogyasztók tettek ki, amelyek nem használtak biometrikus fizetési megoldásokat.

4. Eredmények

Ezen fejezetben bemutatásra kerülnek az adatgyűjtés során érkezett válaszok statisztikai elemzése. Első sorban az összegyűjtött adatok bekódolásra kerültek, Microsoft

Excel segítségével, majd a statisztikai elmezéseket a SmartPLS programban végeztem el. A fejezet során elsőként a leíró statisztikai adatok vannak részletezve, ezt követően pedig a konceptuális modell, illetve a hipotézisek tesztelésére kerül sor.

4.1 Leíró statisztika

Az alábbi alfejezetben bemutatásra kerülnek a minta demográfiai adatai, a fizetési eszközök használata, valamint a nyílt kérdésre érkezett vélemények rövid összefoglalása és elemzése. Az alábbi táblázat ábrázolja a válaszadók demográfiai jellemzőit.

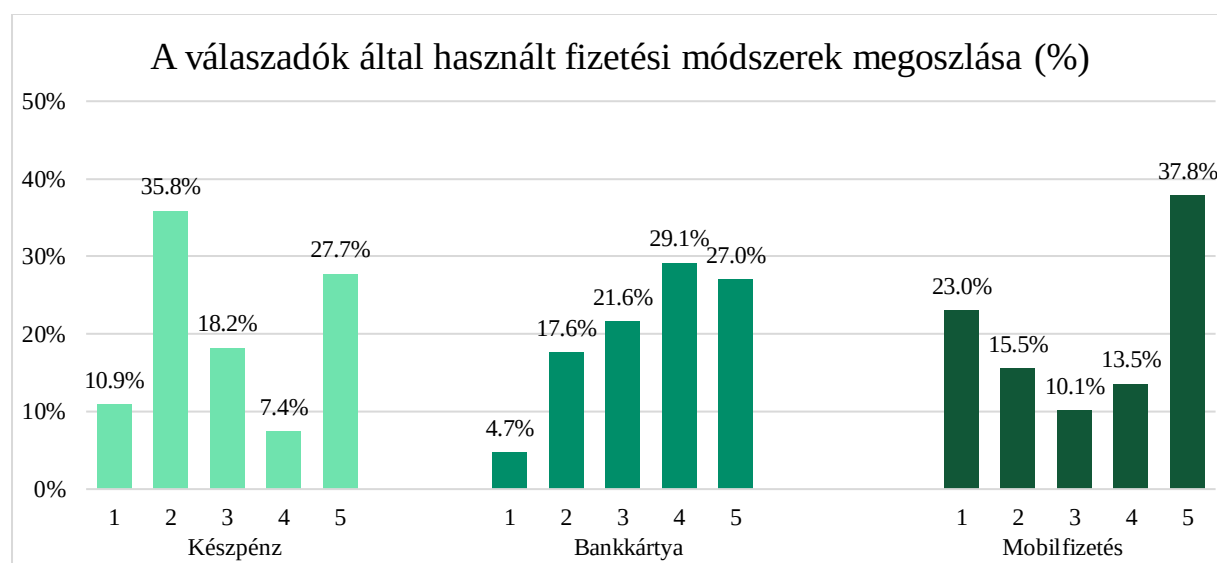
<i>Változó</i>	<i>Kategória</i>	<i>Abszolút gyakoriság (n)</i>	<i>Relatív gyakoriság (%)</i>
Nem	Férfi	58	39,2%
	Nő	90	60,8%
Életkor	18 – 24	56	37,8%
	25 – 34	41	27,7%
	35 – 44	19	12,8%
	45 – 54	17	11,5%
	55 – 64	11	7,4%
	> 65	4	2,7%
Lakhely típusa	Város	100	67,6%
	Vidék	48	32,4%
Legmagasabb iskolai végzettség	Általános iskola	6	4,1%
	Középiskola	46	31,1%
	Egyetemi alapképzés	65	43,9%
	Egyetemi mesterképzés	31	20,9%
Jelenlegi foglalkozás	Diák	41	27,7%
	Alkalmazott	81	54,7%
	Vállalkozó	14	9,5%
	Munkanélküli	5	3,4%
	Nyugdíjas	7	4,7%
Jövedelem	< 2079	50	33,8%
	2080 - 4859	59	39,9%
	> 4859	39	26,4%

Táblázat 1 - A válaszadók demográfiai jellemzői (N=148)

A válaszadók nem szerinti megoszlását tekintve, többségben nők töltötték ki a kérdőívet (60,8%). Az életkor megoszlását illetően, a legtöbb válaszadó 18 és 24 év közötti volt (37,8%), majd ezt követte a 25 és 34 év közöttiek (27,7%), a legkevesebb kitöltés pedig a 65 év feletiek esetében vehető észre (2,7%). A legmagasabb iskolai végzettség a válaszadók körében az egyetemi alapképzés (43,9%), valamint a középiskola (31,1%), a legkevesebb kitöltés az általános iskola esetében merült fel (4,1%). A válaszadók legnagyobb arányban alkalmazott (54,7%), valamint diák (27,7%), a munkanélküliek aránya volt a legalacsonyabb (3,7%). A havi

jövedelem 3 kategóriára volt felosztva: minimálbér alatti (2079 RON), minimálbér (2079 RON) és átlagbér között (2079-4859 RON), illetve átlagbér fellett (>4859 RON). A minimálbér értéke a 2023 október 1-én meghatározott minimálbér értékre vonatkozik, illetve az átlagbér értéke a 2024 januári átlagbérrre vonatkozik, a Ziarul Financiar felméréseire vonatkozva (Roșu, 2024). Így a havi jövedelem szempontjából, a válaszadók legnagyobb része minimálbér és átlagbér közötti jövedelemmel rendelkezik (39,9%), ezt követi a minimálbér alatti jövedelem (33,8%), majd az átlagbér fölötti jövedelemmel rendelkezők aránya 26,4% volt. A válaszadók állandó lakhelyét illetően, a jelentős részük városban él (67,6%), a megyei eloszlást tekintve, Románia 27 megyéjéből érkezett válasz. A legnagyobb arány Kolozs megye esetében észlelhető (54,7%), több mint fele a kitöltőknek Kolozs megyében él. Ezt követte Hargita megye, valamint Szilágy megye (5,8%), majd Maros megye (4,7%).

A továbbiakban bemutatásra kerül, a válaszadók mindennapi vásárlásaik során használt fizetési eszközök aránya.



3 Ábra- A válaszadók által használt fizetési módszerek megoszlása (%)

A fenti diagramm, a válaszadók mindennapi vásárlásaik során történő fizetési módszerek megoszlását mutatja be. Összehasonlítva a 3 fizetési módszert, elmondható, hogy a válaszadók körében, a mobilfizetés a legelterjedtebb (37,8%), valamint a készpénzzel való fizetést, 35,8%-a a kitöltőknek, szinte egyáltalán nem használja. A bankkártyával való fizetés esetében, pedig a válaszadók 29,1%-a szinte teljes mértékben használja a mindennapi vásárlásai során.

A továbbiakban a nyílt kérdésre érkezett válaszok összefoglalása kerül bemutatásra. A válaszadók jelentős része nem említette meg véleményét a biometrikus fizetési megoldások használatáról, így ezen vélemények nem reprezentatívak a teljes mintára tekintve, csupán egy általános képet mutatnak az adott válaszadók véleményéről. A kapott válaszok alapján, kategorizáltam ezen véleményeket.

Az első kategóriát a pozitív vélemények teszi ki. Ezen esetben, a fogyasztók pozitív magatartást mutatnak a biometrikus fizetési megoldások használatával szemben, úgy vélik, hasznos lehet számukra, ugyanis egy gyors megoldást nyújt a mindennapi fizetésekhez *„szerintem nagyon hasznos lenne, gyorsan lehetne fizetni...”*

Pozitív véleményként említették ezen technológia által biztosított kényelmet is, ugyanis nem szükséges pénztárca, valamint számos bankkártya használata *„vagány, nem lenne szükséges pénztárcát vinni a vásárlások során”, „kényelmes lenne szerintem, mert egy ujjérintéssel fizethetnék is”*. Egy további gyakran előfordult pozitív vélemény a biztonság érzetét feltételezte *„biztonságosnak tűnik, nem lophatják le az adataim”*.

A következő kategória a negatív vélemények, amely esetében a válaszadók megemlítették az alacsony elfogadási arányt. Ebben az esetben több válaszadó is megjegyezte, hogy az idősebb korosztály valószínűleg nem alkalmazkodna ezen technológiához *„én élvezném, de szerintem az idősebb generációk biztos nem tudnák használni”*.

Emellett egyes fogyasztók úgy véleik, hogy a biometrikus ismérveken alapuló technológia túlságosan intruzív, kényelmetlen lenne a használata *„érdekes, de kényelmetlen lenne számomra az ilyesmi...” „úgy gondolom kicsit túl intruzív, a személyes szférámat túllépné”*.

Jelentős számú válaszadónak nem sikerült eldöntenie, hogy pozitív vagy negatív véleménnyel rendelkezik a biometrikus fizetési megoldásokról illetve, megemlítésre került, hogy mivel még nem feltétlenül ismerős ezen technológia számukra, emiatt semleges véleményük van *„annyira nem értem mit feltételez, így nincs véleményem” „tetszik is meg nem is” „semleges véleményem van, nem tudom”*.

A nyílt kérdésekre adott válaszok elemzése megtalálható a mellékletekben a Táblázat 4 (A nyílt kérdések elemzésének összefoglalása) alatt.

4.2 Hipotézisek tesztelése

Az alábbi alfejezetben, a konceptuális modell változói közötti kapcsolatok elmezésére, valamint a megfogalmazott hipotézisek tesztelésére kerül sor. Ennek érdekében a SmartPLS programot használtam, a programon belül pedig a PLS-SEM algoritmust. Az elemzés keretén belül megvizsgáltam, hogy a várható teljesítmény (PE), várható erőfeszítés (EE), szubjektív

normák (SN), elősegítő feltételek (FC), hedonikus motiváció (HM), a megszokott viselkedés (HAB), valamint az észlelt pénzügyi kockázat (FR) és az észlelt adavédelmi kockázat (PR) milyen mértékben befolyásolják a biometrikus fizetési megoldások használati szándékát, illetve megvizsgálásra került, ha szignifikáns kapcsolat van köztük vagy sem.

Első lépésként megvizsgáltam, ha a kutatási modell érvényes és megbízható. Ennek érdekében faktorelemzést végeztem, amely során megvizsgált mérőszámokat a mellékletben megtalálható Táblázat 5 (Faktorelemzés során vizsgált mutatók) foglalja össze.

Mivel a faktorelemzés során az összes komponens elérte az ajánlott 0,7-es küszöbértéket (Hair et al, 2020), így egyik komponens sem került kizárára. Így a továbbiakban a faktorelemzés során megalakult konstrukciók érvényességének, valamint megbízhatóságának megvizsgálására került sor. A megbízhatóságot és az érvényességet, az összetétel-megbízhatósági mutató (composite reliability), az AVE (average variance extracted) mutató, illetve a Cronbach's alpha mutató segítségével kerül ellenőrzésre. A Cronbach's alpha mutató értékei minden konstrukció esetében elérték a javasolt 0,7-es értéket, valamint az összetétel-megbízhatósági mutató és az AVE értékek is elérték a 0,7-es küszöbértéket, valamint az AVE esetében a 0,5-ös küszöbértéket (Hair et al, 2020). Ezen mutatók esetében elért értékek, tehát igazolják a modell érvényességét és megbízhatóságát.

Ezt követően lefutattam egy 1000 értékű bootstrapping algoritmust, az útegyütthatók ellenőrzése érdekében. A kapott eredmények az alábbi táblázatban vannak összefoglalva, majd ezen értékek alapján elemzésre kerülnek a változók közötti kapcsolatok, valamint a megfogalmazott hipotézisek tesztelése.

A hipotézisek tesztelését összefoglaló táblázat a mellékletek Táblázat 6 (A hipotézisek tesztelése) található.

A várható teljesítmény (PE) pozitív és szignifikáns hatással van a használati szándékre (UI), így elfogadjuk a H1-et ($p < 0.05$), azaz a várható teljesítmény és a használati szándék között szignifikáns kapcsolat van. Tehát minél nagyobb a fogyasztó által észlelt saját teljesítménye a biometrikus fizetési megoldások használata során, annál inkább jellemző, hogy használni szándékozza ezen fizetési megoldást.

A várható erőfeszítés (EE) és a használati szándék (UI) között nem mutatható ki szignifikáns kapcsolat, ebben az esetben a H2-t elvetjük ($p > 0.05$). Ez alapján a fogyasztók által érzékelt várható erőfeszítés nincs szignifikáns hatással a biometrikus fizetési megoldások használati szándékára.

A szubjektív normák (SN) pozitív és szignifikáns hatással van a használati szándékre (UI), így a H3-t elfogadjuk ($p = 0.070$, amely érték > 0.05 , viszont alacsony mintaszám esetében

a szignifikancia szint 0.1-nél kisebb értékek során is elfogadható – valami hivatkozás). Tehát ez alapján mások véleménye szignifikáns hatással van a biometrikus fizetési megoldások használati szándékára.

Az elősegítő feltételek (FC) és a használati szándék (UI) között nincs szignifikáns kapcsolat ($p > 0.05$), a H4-t elvetjük. Tehát az elősegítő feltételek megléte nem befolyásolja szignifikánsan a biometrikus fizetési megoldások használati szándékát.

A hedonikus motiváció (HM) és a használati szándék (UI) között nem mutatható ki szignifikáns kapcsolat ($p > 0.05$), így a H5-t elvetjük. Ennek értelmében a fogyasztók hedonikus motivációja nincs szignifikáns hatással a biometrikus fizetési megoldások használati szándékával.

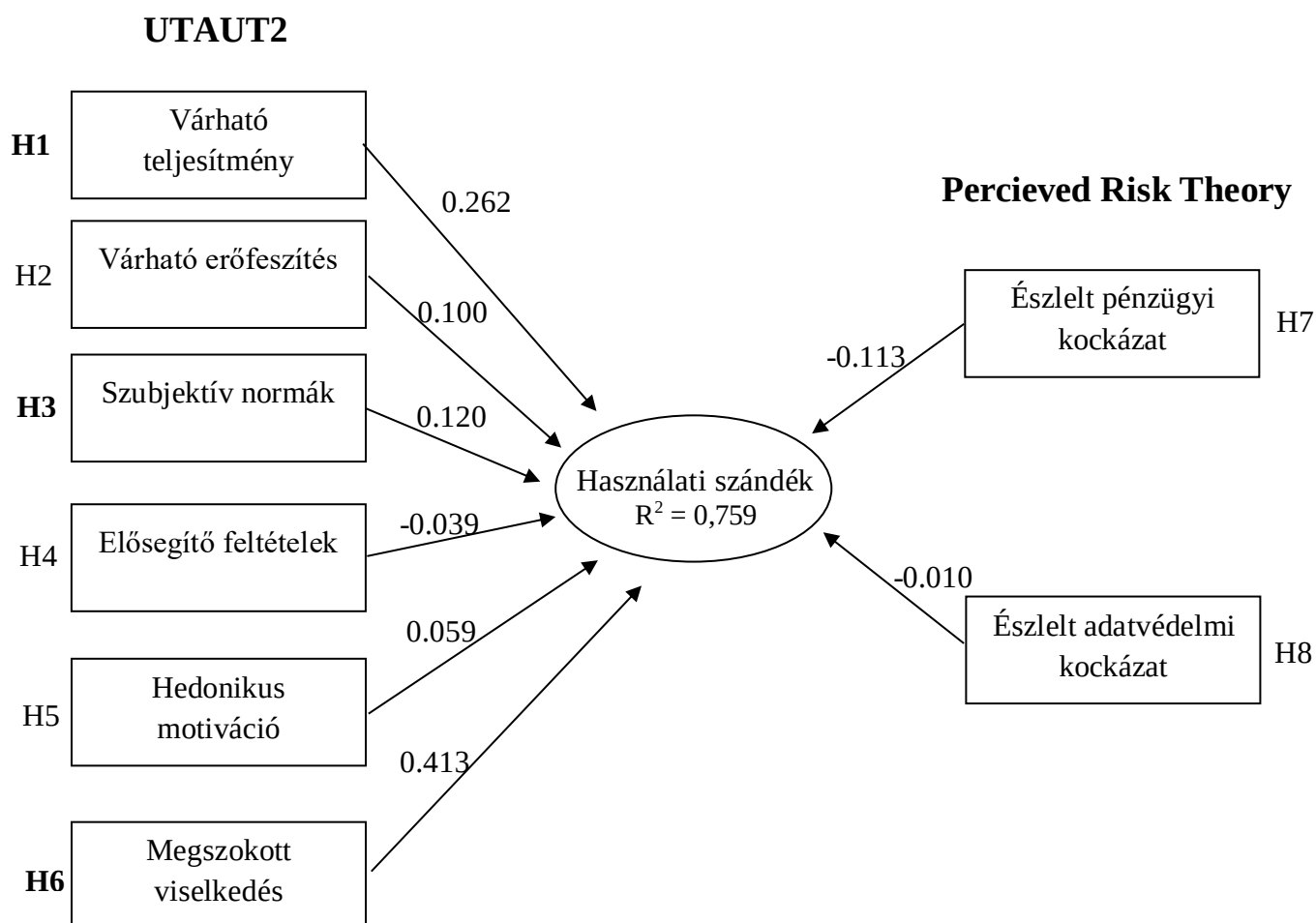
A megszokott viselkedés (HAB) pozitív és szignifikáns hatással van a használati szándékra (UI), így a H6-t elfogadjuk ($p < 0.05$). Ez alapján, ha a biometrikus fizetési megoldások használata megszokottá, természetessé válik, akkor annál inkább nagyobb a fogyasztók használati szándéka ezen fizetési megoldást illetően.

Az észlelt pénzügyi kockázat (FR) és a használati szándék (UI) között nem mutatható ki szignifikáns kapcsolat, így a H7-t elvetjük ($p > 0.05$). A fogyasztók által észlelt pénzügyi kockázat nincs negatív hatással a biometrikus fizetési megoldások használati szándékára.

Az észlelt adatvédelmi kockázat (PR) és a használati szándék (UI) között nincs szignifikáns kapcsolat, elvetjük a H8-at ($p > 0.05$). Az adatok védelmére vonatkozó kockázat nincs negatív befolyással a biometrikus fizetési megoldások használati szándékára.

Az elemzést követően elmondható, hogy a konceptuális modell a biometrikus fizetési megoldások használati szándékának varianciáját 75,9%-ban magyarázza, mivel az $R^2 = 0,759$.

Szignifikánsan a következő változók magyarázzák ezt: a várható teljesítmény (PE) 26,2%-ban magyarázza, a szubjektív normák (SN) 12%-ban magyarázza, valamint a megszokott viselkedés (HAB) 41,3%-ban magyarázza. A további változók esetében nem volt szignifikáns kapcsolat, várható erőfeszítés (EE) 10%; elősegítő feltételek (FC) -3,9%; hedonikus motiváció (HM) 5,9%; észlelt pénzügyi kockázat (FR) -11,3%; észlelt adatvédelmi kockázat (PR) -1%.



4 Ábra- A konceptuális modell tesztelésének eredménye

Az fenti ábra, az elemzéseket követően, a konceptuális modell tesztelésének eredményeit mutatja be.

5. Következtetések

A kutatás fő céljához igazodva, megvizsgálásra került a biometrikus fizetési megoldások használati szándéka, valamint elfogadása a romániai fogyasztók körében. A kutatásban felhasznált minta nem tekinthető reprezentatívnak, mivel alacsony számú kitöltés érkezett, valamint a minta összetétele nem volt arányos. Így a kapott eredmények és következtetések nem általánosíthatóak a romániai fogyasztókra, kizárólag a kutatásban felhasznált mintára jellemzőek.

Az első kutatási kérdés, arra kereste a választ, hogy melyek azok a tényezők, amelyek hatnak a fogyasztók biometrikus fizetési megoldások elfogadására és használati szándékára.

Ezen kutatási kérdés megválaszolása érdekében a biomterikus fizetési megoldásokra vonatkozó szakirodalomban használatos UTAUT 2 modell 6 eleme került megvizsgálásra.

A hipotézistesztelés során, kiderült, hogy jelen kutatásban csupán három változónak van szignifikáns hatása a használati szándékra. Az első változó, amely pozitív, szignifikáns kapcsolatban van a felhasználási szándékkal az elvárt teljesítmény (PE). Tehát, minél inkább elősegíti ezen technológia használata a fogyasztók teljesítményét, beleértve például a gyors fizetés lehetőségét, annál inkább lesz jellemző a használata. Ezen esetben Liébana-Cabanillas et al. (2024) kutatásában meglévő eredmények megegyeznek jelen kutatás eredményeivel, ugyanis az egyik legjelentősebb befolyásoló tényező a biometrikus fizetési módszerek használati szándékára a fogyasztók által elvárt teljesítmény volt.

Egy további változó, amely szignifikáns hatást fejt a használati szándékra (UI) a szubjektív normák (SN). Ennek értelmében a fogyasztók használati szándékát befolyásolja más, fontos személyek véleménye, valamint olyan személyek, amelyek véleménye fontosnak számít a fogyasztók számára. Ezen változó Zarco et al. (2024) kutatásában is jelentős hatással bír a használati szándékra, valamint Liébana-Cabanillas et al. (2024) kutatásában is szignifikáns kapcsolat mutatható meg, viszont gyengébb hatás volt észrevehető a többi változóhoz képest.

A harmadik változó, amely szignifikáns kapcsolatban van a használati szándékkal (UI), a megszokott viselkedés (HAB). Ezen változó esetében merül fel a legerősebb pozitív és szignifikáns kapcsolat. Tehát, minél inkább megszokottá, természetessé válik ezen fizetési technológia, annál inkább jellemző, hogy a fogyasztók használni fogják. Ugyan Liébana-Cabanillas et al. (2024) kutatásában is szignifikáns kapcsolat vehető észre, ezen változó gyenge hatást gyakorol a használati szándékra, ellentétbe a jelen kutatással, ahol ezen változó rendelkezik a legerősebb kapcsolattal.

A további változók: a várható erőfeszítés (EE), az elősegítő feltételek (FC), illetve a hedonikus motiváció (HM) nincsenek szignifikáns hatással a használati szándékra (UI). Tehát, jelen mintában a fogyasztók által érzékelt erőfeszítés, azaz milyen mértékben egyszerű az adott technológia használata nem befolyásolja a használati szándékot. Ezen eredmény jelentősen eltér a szakirodalomban említett eredményektől, ugyanis Liébana-Cabanillas et al. (2024) kutatása során a várható erőfeszítés az egyik legerősebb szignifikáns hatással van a használati szándékra. Továbbá jelen kutatás esetében az elősegítő feltételek (FC), mint például a technológiához szükséges erőforrások megléte (ismeretek, okoseszközök stb.) nincs szignifikáns hatással ezen technológia használati szándékára. A nyílt kérdésekre kapott válaszok alapján, kiderült, hogy számos kitöltő nem tudja pontosan, hogy mit feltételez ezen

technológia, így valószínűleg nem érzékelt, hogy például milyen ismeretekkel kell rendelkezni a biometrikus fizetés során. A szakirodalomban szignifikáns kapcsolat jelenik meg ezen változó esetében (Liébana-Cabanillas et al., 2024). Az utolsó változó, amely jelen kutatásban nincs szignifikáns hatással a használati szándékra (UI) a hedonikus motiváció. Tehát a fogyasztók által érzékelt izgalom, szórakozás ezen technológia használata során, nincs szignifikáns hatással a használati szándékra, a szakirodalommal bemutatott eredményekkel szembe, ahol szignifikáns hatás észlelhető (Liébana-Cabanillas et al., 2024).

A második kutatási kérdés arra kereste a választ, hogy melyek azok a kockázati tényezők, amelyek negatív hatással vannak a fogyasztók biometrikus fizetési megoldások elfogadására és használati szándékára.

Ezen esetben egyik változó sem volt szignifikáns hatással a használati szándékra (UI). Tehát a fogyasztók által észlelt pénzügyi kockázat (FR) nincs negatív hatással a használati szándékra, ennek ellenére használatra kerülne ezen technológia a fogyasztók körében. Továbbá az észlelt adat védelem esetében sem jelenik meg szignifikáns kapcsolat, így ezen változó sincs negatív hatással a használati szándékra. Ezzel ellentétben a szakirodalomban az innovatív fizetési megoldások kontextusában a két legerősebb szignifikáns kapcsolat vehető észre (Yang et al., 2015; Reepu & Arora, 2022). Kiegészítve a nyílt kérdésre érkező válaszokkal, a kitöltők összességében egy biztonságos fizetési megoldásként tekintenek a biometrikus fizetésre, így feltételezhető, hogy nem érzékelnek kockázatot.

Összességében, az elemzések során kapott eredmények, arra mutatnak rá, hogy a biometrikus fizetési megoldások elfogadására és használati szándékára szignifikáns hatással a megszokott viselkedés, a várható teljesítmény, valamint a szubjektív normák vannak. A legerősebb hatással pedig a megszokott viselkedés említhető meg. Így tehát minél megszokottabbá válik ezen fizetési technológia, annál inkább lesz használatos a fogyasztók körében. Továbbá minél inkább hasznosnak bizonyul, elősegíti a fogyasztó teljesítményét, annál inkább lesz jellemző a használata, valamint mások véleménye is meghatározó a használati szándékra és elfogadásra.

Az észlelt kockázatokat tekintve, a pénzügyi, valamint az adatvédelmi észlelt kockázatok nem hatnak negatívan a fogyasztók használati szándékára.

Jelen kutatás hozzájárul a biometrikus fizetési megoldások használati szándékának jobb megértéséhez, illetve azon tényezők megismeréséhez, amelyek befolyásolják ezen innovatív fizetési módszer használatát.

5.1 A kutatás korlátai

A kutatás fő korlátját az alacsony mintaszám teszi ki, valamint a minta aránytalan demográfiai eloszlása. A kérdőívet nagyrészt nők töltötték ki, valamint egyetemi hallgatók, fiatalabb generációba tartozó személyek, így a minta nem tekinthető reprezentatívnak.

Egy másik jelentős korlátot képezi, azon tény, hogy a kitöltők nem értelmezték helyesen a biometrikus fizetés meghatározását, így torzultak az eredmények. Bár a kérdőív leírásában magyarázatra került a biometrikus fizetési megoldás, nem volt elég egyértelmű a kitöltők számára mit feltételez ezen technológia. Ebből adódóan összekeverték, más fizetési módszerekkel, valamint különféle eszközök és alkalmazások feloldásához használt biometrikus technológiával, például az okostelefon feloldása vagy egy alkalmazásba való belépéssel. A félreértelmezés elkerülése érdekében, a tesztelés során célszerű lett volna több személy megkérdezése, illetve egy részletesebb magyarázat megadása. Emellett a biometrikus fizetési megoldások általánosságban kerültek felmérésre, így feltételezhető, hogy a válaszadók különféle típusú biometrikus fizetési megoldásokra gondoltak a kitöltés során.

Egy további korlát, az időkorlát volt. Időhiány miatt az adatgyűjtés 5 napot tartott. Valószínűleg, ha egy hosszabb periódusig folyt volna az adatgyűjtés, a minta nagysága is növekedett volna. Így tehát egy reprezentatívabb minta alakulhatott volna meg.

Egy következő korlát, a kutatásban használt mintavételi eljárás, az adagyűjtés során a hólabda módszert alkalmaztam, amely segítségével többnyire ismerősi köreimből származó kitöltések érkeztek.

Egy utolsó korlátot jelképezett a korlátozott számú kutatások, valamint statisztikai adatok, információk ezen témával kapcsolatban, mivel viszonylagosan egy új, feltörekvő technológiáról van szó.

5.2 További kutatási lehetőségek

További kutatási lehetőségként, különböző demográfiai változók alapján lehetne vizsgálni a biometrikus fizetési megoldások elfogadását és használati szándékát, mint például megfigyelni, hogy a különböző korcsoportok, generációk milyen mértékben használnák ezen technológiát, valamint összehasonlítani ezen korcsoportok közötti különbségeket.

Továbbá, különféle pszichográfiai tényezők megvizsgálása is egy további kutatási lehetőséget jelentene. Például az egyének személyiségjegyeinek megfigyelése és ezen hatásának elemzése a biometrikus fizetési megoldások használatának szándékára. Egy másik kutatási

lehetőség, a személyek innováció elfogadási szintjének mérése, illetve azon szint milyen mértékben befolyásolja ezen technológia használatát.

Emellett felmérésre kerülhetne, hogy a különböző szektorokban alkalmazott személyek, milyen mértékben lennének hajlandók használni ezen technológiát.

Mivel jelen kutatás általánosan vonatkozott a biometrikus fizetési lehetőségekre, érdemes lenne a különféle típusainak vizsgálata. Fókuszálva, például a biometrikus bankkártya, valamint a biometrikus mobilfizetés használatára. Emellett a különféle biometrikus ismérvekkel való fizetés elfogadása és használati szándéka is egy kutatási lehetőséget jelképez, például megfigyleni külön-külön, hogy az ujjlenyomattal vagy az arcfelismeréssel való fizetés milyen mértékben kerülne használatra.

5.3 Gyakorlati jelentőség és javaslatok

A kutatásom eredményei nem általánosíthatóak, az alacsony minta szám miatt, viszont a kapott eredmények, gyakorlati jelentőséget képezhetnek a pénzügyi szektorhoz tartozó vállalatok számára, főként a bankok esetében. Emellett kereskedelmi egységeknek is hasznos információkat szolgálhatnak, továbbá a biometrikus fizetési szoftvereket, hardvereket gyártó vállalatok számára is felhasználhatóak ezen eredmények.

Elsőként az eredmények alapján a fogyasztók számára fontos, hogy ezen fizetési megoldások hasznosnak bizonyuljanak, optimalizálják ezen fogyasztók teljesítményérzetét. Így a software, valamint hardware gyártó vállalatoknak, külön figyelniük kell a rendszerek kialakítása során, arra, hogy gyorsnak bizonyuljanak, valamint elősegítsék a fogyasztók produktívítási szintjét, például gyors fizetés.

Továbbá, mivel a fogyasztók számára ezen technológia, újnak, ismeretlennek minősül, így bevezetésének kezdetében, a bankok valamint a kereskedelmi egységek marketingkommunikációs stratégiájuk során edukációs, valamint informatív jellegű tartalmakkal szólíthatnák meg a fogyasztókat. Például a kereskedelmi egységek esetében rövid videók segítségével bemutatásra kerülhetne ezen fizetési módszer használata, valamint a fizetési terminálok körül informatív jellegű információk szemléltetése lenne hasznos. Továbbá a fogyasztók számára, fontosnak bizonyosult más személyek véleménye a használati szándékra, az elvárt teljesítmény, valamint a megszokott viselkedés, így a marketingkommunikáció során, a biometrikus fizetési lehetőségek népszerűsítése érdekében, hangsúlyt lehetne fektetni ezen tényezőkre. Példaként megemlíteném az olyan tartalmak gyártását, amelyek kiemelik ezen technológia haszosságát, valamint bemutatják, hogy ezen

fizetési megoldás természetessé válhat. Emellett az olyan jellegű tartalmak gyártását, amelyekben fontos személyek, például baráti vagy családi szerepkörök kerülnek bemutatásra, ajánlva ezen technológiát a hozzájuk közel álló személyeknek, valamint ennek magyarázatát szemléltetik.

Irodalomjegyzék

Ajzen, I. (1991), The theory of planned behavior, *Organizational behavior and human decision processes*, 50(2), 179-211.

Ajzen, I., & Fishbein, M. (1980), *Understanding attitudes and predicting social behavior*. Prentice Hall.

Akhtar, Z., Micheloni, C., & Foresti, G. L. (2015), Biometric liveness detection: Challenges and research opportunities, *IEEE Security & Privacy*, 13(5), 63-72.

Babisch, A. (2012), *Biometric Authentication*. Types of biometric identifiers, p. 2-53

Bolle, R. M., Connell, J. H., Pankanti, S., Ratha, N. K., & Senior, A. W. (2004), *Guide to biometrics*. Springer Science & Business Media, New York.

Clodfelter, R. (2010), Biometric technology in retailing: Will consumers accept fingerprint authentication?, *Journal of Retailing and Consumer Services*, 17(3), 181-188.

Davis, F. D., Bagozzi, R. P., & Warshaw, P. R. (1989), User acceptance of computer technology: A comparison of two theoretical models, *Management science*, 35(8), 982-1003.

emarketer.com, (2019), *How Do Consumers Feel About Biometrics* <https://www.emarketer.com/content/how-do-consumers-feel-about-biometrics>, megnyitva: 2024.04.27

Factmr.com (2022), *Biometric Payment Market Outlook*, <https://www.factmr.com/report/1850/biometric-payment-market>, megnyitva: 2024.04.30

gdpr-info.eu, <https://gdpr-info.eu/art-9-gdpr/>, megnyitva: 2024.04.26.

Hair Jr, J. F., Howard, M. C., & Nitzl, C. (2020), Assessing measurement model quality in PLS-SEM using confirmatory composite analysis, *Journal of business research*, 109, 101-110.

Hwang, J., Kim, J. S., Kim, H. M., & Kim, J. J. (2024), Effects of motivated consumer innovativeness on facial recognition payment adoption in the restaurant industry: A cross-cultural study, *International Journal of Hospitality Management*, 117, 103646.

Imbrea, A., (2018), *Auchan Romania și Oney Bank au lansat Well.com, primul sistem de plata biometric implementat de un comerciant în România*, wall-street.ro, <https://www.wall-street.ro/articol/Companii/237306/auchan-romania-si-oney-bank-au-lansat-well-com-primul-sistem-de-plata-biometric-implementat-de-un-comerciant-in-romania.html#gref>, megnyitva: 2024.04.28

Jung, J. (2021), *What are Salted Passwords and Password Hashing?*, okta.com, <https://www.okta.com/blog/2019/03/what-are-salted-passwords-and-password-hashing/>, megnyitva: 2024.04.26.

Kim, M., Kim, S., & Kim, J. (2019), Can mobile and biometric payments replace cards in the Korean offline payments market? Consumer preference analysis for payment systems using a discrete choice model, *Telematics and Informatics*, 38, 46-58.

Kodituwakku, S. R. (2015), Biometric authentication: A review, *Int. J. Trend Res. Dev*, 2, 113-123.

Kumar, D., & Ryu, Y. (2009), A brief introduction of biometrics and fingerprint payment technology, *International Journal of Advanced Science and Technology*, 3, p. 185-192

Kumar, D., Ryu, Y., & Kwon, D. (2008), A survey on biometric fingerprints: The cardless payment system, *International Symposium on Biometrics and Security Technologies*, p. 1-6

Liébana-Cabanillas, F., Kalinic, Z., Muñoz-Leiva, F., & Higuera-Castillo, E. (2024), Biometric m-payment systems: A multi-analytical approach to determining use intention, *Information & Management*, 61(2), 103907.

Lindner, J. (2022), *Biometric Statistics: Market Report & Data*, gintux.com, <https://gintux.org/biometric-statistics/>, megnyitva: 2024.04.30

Malhotra K. N., & Simon, J. (2017), Marketingkutatás. Akadémiai Kiadó. https://mersz-hu.web.bcucuj.ro:2443/dokumentum/dj198mk_72

Malone, C. (2023), juniperresearch.com, <https://www.juniperresearch.com/research/fintech-payments/fraud-identity/global-biometric-in-store-payments-market/>, megnyitva: 2024.04.30

Manisha, & Kumar, N. (2020), Cancelable biometrics: a comprehensive survey, *Artificial Intelligence Review*, 53(5), 3403-3446.

mastercard.us, *Driving hardholder security and convinience* <https://www.mastercard.us/en-us/business/overview/safety-and-security/authentication-services/biometrics/biometrics-card.html>, megnyitva: 2024.04.28

Moriuchi, E. (2021), An empirical study of consumers' intention to use biometric facial recognition as a payment method, *Psychology & Marketing*, 38(10), 1741-1765.

Mróz-Gorgoń, B., Wodo, W., Andrych, A., Caban-Piaskowska, K., & Kozyra, C. (2022), Biometrics innovation and payment sector perception, *Sustainability*, 14(15), 9424.

nttdatipay.com, (2024), *Biometric Payment System: Everything You Should Know*, <https://www.nttdatipay.com/blog/biometric-payment-system/>, megnyitva: 2024.04.30

Ogbanufe, O., & Kim, D. J. (2018), Comparing fingerprint-based biometrics authentication versus traditional authentication methods for e-payment, *Decision Support Systems*, 106, p. 1-14.

Othman, A., *What are the advantages and disadvantages of biometrics*, gbgplc.com, <https://www.gbgplc.com/en/blog/what-are-the-advantages-and-disadvantages-of-biometrics/>, megnyitva: 2024.04.30

Pascu, L., (2020), *Global Biometrics Market to Reach \$71.6B by 2024 on Demand for Emerging Tech: Report*, biometricupdate.com, [Global biometrics market to reach .6B by 2024 on demand for emerging tech: report | Biometric Update](https://biometricupdate.com/global-biometrics-market-to-reach-6B-by-2024-on-demand-for-emerging-tech-report), megnyitva: 2024.04.30

payeye.com, *About PayEye* <https://payeye.com/about-payeye/>, megnyitva: 2024.04.30

refaces.com, (2021), *Biometric authentication, identification, and verification in 2021*, <https://refaces.com/articles/biometric-authentication-identification#1>, megnyitva: 2024.04.26.

Reepu, R. A., & Arora, R. (2022), The Effect of Perceived Risk on Intention to Use Online Banking, *Universal Journal of Accounting and Finance*, 10(1), 62-71.

Roșu, R. (2024), *Salariul mediu net lunar a coborât în prima luna din 2024*, <https://www.zf.ro/zf-24/salariul-mediu-net-coborat-prima-luna-2024-4-859-lei-220-lei-nivelul-22293263>, zf.ro, megnyitva: 2024.04.22

Sreekumar, S. (2010), Biometric Authentication in Mobile Payments

Tamilmani, K., Rana, N. P., Wamba, S. F., & Dwivedi, R. (2021), The extended Unified Theory of Acceptance and Use of Technology (UTAUT2): A systematic literature review and theory evaluation, *International Journal of Information Management*, 57, 102269.

theguardian.com, (2019), *Smile-to-Pay: Chinese shoppers turn to facial payment technology*, <https://www.theguardian.com/world/2019/sep/04/smile-to-pay-chinese-shoppers-turn-to-facial-payment-technology>, megnyitva: 2024.04.30

Venkatesh, V., Morris, M. G., Davis, G. B., & Davis, F. D. (2003), User acceptance of information technology: Toward a unified view, *MIS quarterly*, 425-478.

Venkatesh, V., Thong, J. Y., & Xu, X. (2012), Consumer acceptance and use of information technology: extending the unified theory of acceptance and use of technology, *MIS quarterly*, 157-178.

visa.navigate.com, *How Biometric Authentication is Revolutionizing Payment Experiences*, <https://navigate.visa.com/cemea/money-movement/watch-video-how-biometric-authentication-is-revolutionizing-payment-experiences/>, megnyitva: 2024.04.30

Yang, Y., Liu, Y., Li, H., & Yu, B. (2015), Understanding perceived risks in mobile payment acceptance, *Industrial Management & Data Systems*, 115(2), 253-269.

Zarco, C., Giráldez-Cru, J., Cordon, O., & Liébana-Cabanillas, F. (2024), A comprehensive view of biometric payment in retailing: A complete study from user to expert, *Journal of Retailing and Consumer Services*, 79, 103789.

Mellékletek

Biometrikus jellemzők		
Fizikai jellemzők	Viselkedésbeli jellemzők	Kombinált jellemzők
Ujjlenyomat	Járásmód	Hang/Beszéd
Tenyérlenyomat	Billentyűleütés	Aláírás
Kéz geometria	P300 agyhullámok mozgása	Kézírás
Arc geometria		
Fül alak		
Írisz mintázat		
Retina mintázat		
Vérerek mintázata		
DNS		

Tablázat 1 - A biometrikus jellemzők osztályozása

<i>Szerzők és publikáció éve</i>	<i>Minta</i>	<i>Vizsgált technológia</i>	<i>Használt elmélet(ek)</i>	<i>Fő eredmények</i>
Yang et al. (2015)	Kína 310 kitöltő	Mobilfizetés	Bizonytalansági- kockázat érték keretrendszer (Észlelt kockázat elmélet+ Kilátáselmélet+ Észlelt értékelmélet)	FR → UI: erős szignifikáns kapcsolat PR → UI: erős szignifikáns kapcsolat
Reepu & Arora (2022)	India 226 női kitöltő	Online banking	Észlelt kockázat elmélet	PR → UI: erős szignifikáns kapcsolat
Liébana- Cabanillas et al. (2024)	Spanyolország 2586 okostelefon felhasználó	Biometrikus mobilfizetés PayEye alkalmazás	UTAUT2 Észlelt kockázat elmélet	PE → UI: erős szignifikáns kapcsolat EE → UI: erős szignifikáns kapcsolat HM → UI: erős szignifikáns kapcsolat Észlelt kockázat → UI: erős szignifikáns kapcsolat
Zarco et al. (2024)	Spanyolország 1905 kitöltő 20 FinTech szakértő	Biometrikus bankkártya	UTAUT2 Általános észlelt kockázat elmélet Észlelt bizalom elmélet	Észlelt kockázat → UI: erős szignifikáns kapcsolat Észlelt bizalom → UI: erős szignifikáns kapcsolat SN → UI: erős szignifikáns kapcsolat

Tablázat 2 - Áttekintett kutatások összefoglalása

<i>Változók</i>		<i>Komponens</i>	<i>Forrás</i>
Várható teljesítmény (Performance Expectancy) – PE	PE1	A biometrikus fizetési megoldások használata hasznosnak bizonyulna a mindennapjaim során.	
	PE2	A biometrikus fizetési megoldások használata segítene a tranzakciók gyorsabb lebonyolításában.	Liébana-Cabanillas et al., 2024
	PE3	A biometrikus fizetési megoldások használata növelné a produktivitási szintem.	
Várható erőfeszítés (Effort Expectancy) – EE	EE1	Könnyen megtanulható lenne a biometrikus fizetés használata.	
	EE2	A biometrikus használata világos és érthető lenne.	
	EE3	A biometrikus fizetéshez szükséges készségeket könnyen elsajátítanám.	Liébana-Cabanillas et al., 2024
	EE4	Könnyűnek találnám a biometrikus fizetés használatát.	
Szubjektív normák (Subjective Norms) – SN	SN1	A számomra fontos személyek szerint, kellene biometrikus fizetési megoldásokat használnom.	
	SN2	A számomra fontos személyek egyet értenének azzal, ha biometrikus fizetési módszereket használnék.	Liébana-Cabanillas et al., 2024
	SN3	A számomra fontos személyek elvárják tőlem, hogy biometrikus fizetési módszereket használjak.	
	SN4	A legtöbb személy, akinek a véleményét értékelem, úgy gondolja, hogy kellene biometrikus fizetési megoldásokat használnom.	
Elősegítő feltételek (Facilitating Conditions) – FC	FC1	Rendelkeznék a biometrikus fizetéshez szükséges erőforrásokkal.	
	FC2	Rendelkeznék a biometrikus fizetéshez szükséges ismeretekkel.	
	FC3	Segítséget kaphatnék másoktól, ha nehézségeim lennének a biometrikus fizetés használatával.	Liébana-Cabanillas et al., 2024
Hedonikus motiváció (Hedonik motivation) – HM	HM1	A biometrikus fizetés használata izgalmas lenne.	
	HM2	A biometrikus fizetés használata nagyon szórakoztató lenne.	Liébana-Cabanillas et al., 2024
	HM3	Élvezném a biometrikus fizetés használatát.	
Megszokott viselkedés (Habit) – HAB	HAB 1	A biometrikus fizetés használata szokássá válna számomra.	Liébana-Cabanillas et al., 2024
	HAB 2	Úgy érzem, muszáj lenne használnom a biometrikus fizetést.	
	HAB 3		
Észlelt pénzügyi kockázat (Perceived Financial Risk) - PR	PR1	A bankszámlámra vonatkozó adatok kiszolgáltatottak lennének, abban az esetben, ha használnám a biometrikus fizetést.	
	PR2	Nagy esély van pénzügyi veszteségre, abban az esetben, ha használnám a biometrikus fizetést.	Yang et al., 2015
	PR2	Indokolatlan díjakat vonnának le, abban az esetben, ha használnám a biometrikus fizetést.	

Észlelet adatvédelmi kockázat (Perceived Privacy Risk) - PR	PR1	Nagy esély van arra, hogy a személyes adataim nem kívánt célokból is fellelnének használva, abban az esetben, ha használnám a biometrikus fizetést.	Yang et al., 2015
	PR2	A személyes adataim nem megfelelően lennének megosztva és eladhatják őket, abban az esetben, ha használnám a biometrikus fizetést.	
	PR3	A személyes adataimhoz más, nem kívánt személyek is könnyen hozzáférhetnének, abban az esetben, ha használnám a biometrikus fizetést.	
Használati szándék (Use Intention) - UI	UI1	Feltételezve, hogy hozzáférnék a biometrikus fizetéshez, szándékomban állna használni vásárlásaim során.	Liébana-Cabanillas et al., 2024
	UI2	Feltételezve, hogy hozzáférnék a biometrikus fizetéshez, a következő néhány hónapban használnám vásárlásaim során.	
	UI3	Feltételezve, hogy hozzáférnék a biometrikus fizetéshez, szándékomban állna rendszeresen használni vásárlásaim során.	

Táblázat 3 - Kérdőív szerkezete

Pozitív magatartás	Gyorsaság
	Kényelem
	Biztonság
Negatív magatartás	Nehéz elfogadás
	Intruzív
Semleges magatartás	Tartózkodás

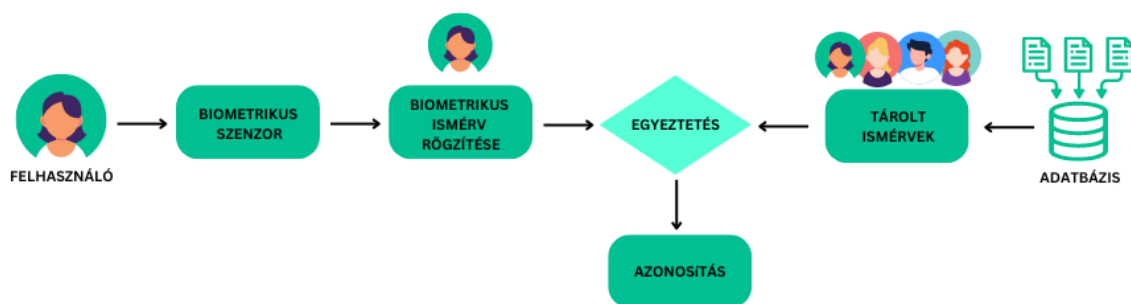
Táblázat 4 - A nyílt kérdések elemzésének összefoglalása

<i>Faktor</i>	<i>Komponens</i>	<i>Faktorsúlyok</i>	<i>Cronbach's alfa</i>	<i>Composite reliability</i>	<i>Average variance extracted (AVE)</i>
PE	PE1 PE2 PE3	0.945 0.945 0.921	0.931	0.931	0.878
EE	EE1 EE2 EE3 EE4	0.909 0.903 0.904 0.931	0.933	0.943	0.831
SN	SN1 SN2 SN3 SN4	0.876 0.761 0.813 0.902	0.859	0.868	0.705
FC	FC1 FC2 FC3	0.837 0.798 0.869	0.785	0.803	0.697
HM	HM1 HM2 HM3	0.938 0.936 0.962	0.940	0.943	0.894
HAB	HAB1 HAB2 HAB3	0.913 0.931 0.849	0.880	0.885	0.807
FR	FR1 FR2 FR3	0.892 0.922 0.838	0.860	0.863	0.783
PR	PR1 PR2 PR3	0.904 0.950 0.953	0.931	0.983	0.876
UI	UI1 UI2 UI3	0.963 0.953 0.956	0.954	0.954	0.916

Táblázat 5 - Faktorelemzés során vizsgált mutatók

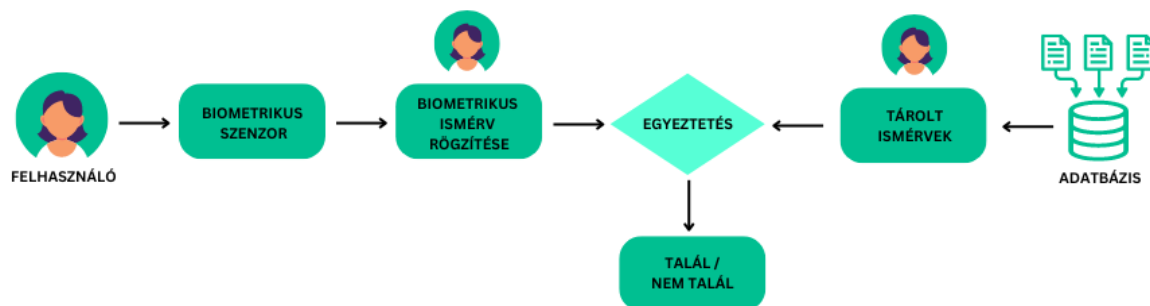
Hipotézisek	Útegyüttható (path coefficient)		Szórás	T-statisztika	P-érték	Kapcsolat
	Eredeti minta	Mintaátlag				
H1 PE→UI	0.262	0.263	0.086	3.064	0.002	Van
H2 EE → UI	0.100	0.099	0.082	1.233	0.218	Nincs
H3 SN→UI	0.120	0.117	0.066	1.814	0.070	Van
H4 FC→UI	-0.039	-0.034	0.054	0.711	0.477	Nincs
H5 HM→UI	0.059	0.065	0.123	0.483	0.629	Nincs
H6 HAB→UI	0.413	0.406	0.100	4.138	0.000	Van
H7 FR→UI	-0.113	-0.115	0.070	1.618	0.106	Nincs
H8 PR→UI	-0.010	-0.009	0.061	0.166	0.868	Nincs

Táblázat 6 - A hipotézisek tesztelése



Ábra 1 – Identifikációs folyamat

Forrás: Manisha & Kumar, 2020, 1. o. alapján, saját szerkesztés



Ábra 2 – Verifikációs folyamat

Forrás: Manisha & Kumar, 2020, 1. o. alapján, saját szerkesztés

1. Melléklet – Biometrikus rendszerek működésének leírása

Ujjlenyomat alapú azonosítás: Az egyik legnépszerűbb és legrégebbi biometrikus azonosítási forma az ujjlenyomat beolvasása (Kodituwakku, 2015). Ezen azonosítási módszert a szakirodalomban daktiloszkópiának is nevezik (Babisch, 2012). Az ujjlenyomatot képző minták egyediek, az egypetéjű ikrek esetében is, így meghatározható egy egyén személyazonossága (Kumar & Ryu, 2009). Az ujjlenyomatot beolvasó rendszerek az ujjbegyeken levő barázdákat osztályozzák, olyan mikroszkópikus részletek szerint, mint például a barázdák végpontjai és elágazásai (Kumar & Ryu, 2009), továbbá vizsgálják az íveket és hurkokat is (Sreekumar, 2010), valamint egyes technológiák a barázdák közötti pórusokat is felméri (Kumar & Ryu, 2009).

Az ujjlenyomatok beolvasása már több, mint száz éve jelen van az igazságszolgáltatásban, az egyik legfeljetebb és legpontosabb azonosítási módszer, valamint ezen rendszerek a legolcsóbbak közé sorolhatóak. Emellett az egyik legegyszerűbben használható biometrikus technológia (Clodfelter, 2010), valamint szinte azonnali hozzáférést nyújt egy adott rendszerhez (Kumar & Ryu, 2009). Napjainkban világszerte a legsűrűbben használt biometrikus azonosítási módszer (Liébana-Cabanillas et al., 2024).

Tenyérnyomat és kéz geometria alapú azonosítás: A tenyérnyomat a kezek tenyér részéről beolvasott képet jelképezi. Ezen lenyomat is könnyen megkülönböztethető és beolvasható különböző eszközökkel, hasonlóan az ujjlenyomat beolvasó technológiákhoz. A tenyér mintázata három fő elemből tevődik össze: elsődleges vonalak, másodlagos vonalak,

valamint barázdák. Két tenyér mintázatának összehasonlítása során, olyan információk is figyelembe vannak véve, mint például a bemélyedések és a bőr textúrája (Babisch, 2012).

A kézgeometria esetében, a teljes kéz mérete és formája beolvasásra kerül (Clodfelter, 2010). Az azonosítás érdekében a rendszer olyan jellemzőket mérhet, mint például a kéz vagy az ujjak szélessége, hosszúsága, illetve a kéz felületének nagysága (Kumar & Ryu, 2009). A kéz beolvasására használt szkennelő rendszerek nagyon pontosak, azonban viszonylag drágák (Clodfelter, 2010).

Arcfelismerésen alapuló azonosítás: Egy személy arcának megtekintése a legegyszerűbb módja egy adott személy felismeréséhez. Az arcfelismerést, hagyományos, nem biometrikus technológiát alkalmazva, számos területen használatra kerül, például a jogosítvány, a személyazonosító igazolvány, illetve egyes bankkártyák esetében. Ezen helyzetben csupán egy kép készül a felhasználóról (Sreekumar, 2010).

Az arcfelismerő technológiák egy egyén különböző arcvonásait elemzi (Clodfelter, 2010). Az ember arcát illetően, számos megkülönböztethető pont létezik, 80 csomópontot azonosít be az arc IT, ezen pontok pedig különböző képpen mérhetőek, például a szemek közötti távolsági pontok, a szemgödör mélysége, az orr szélessége, az arccsontok alakja, valamint az állkapocsvonal hosszúsága. Ezen csomópontok mérését követően, a rendszer létrehoz egy numerikus kódot, amely az arclenyomatot képezi az adatbázisban. A használt rendszerektől függően történhet 2D vagy 3D mérés (Babisch, 2012).

Az arcfelismerés világszerte a második leghasználtabb biometrikus technológia, az ujjlenyomatot követően (Liébana-Cabanillas et al., 2024).

Írisz felismerésen alapuló azonosítás: Az írisz, a szemben található színes rész, amely körülveszi a pupillát. Jelen biometrikus technológia arra alapozódik, hogy minden egyén szemében található írisz mintázat és szín egyedi, így ezen összetett szerkezet hozzájárul a jellemzők összehasonlításához (Kodituwakku, 2015). Az írisz jellemzői körülbelül 10-60 cm távolságtól is beolvashatóak, a mérés során az egyén, nyugodt állapotban, egy kamerába kell nézzen, ameddig befejeződik az elemzés (Clodfelter, 2010).

A szakértők véleménye szerint az írisz mintázata egyedibb, mint a hópelyhek mintázata, így az egyik leígéretesebb eszközök közé sorolható. Az írisz beolvasása során, egy digitális kamera segítségével egy kép készül a szemről, illetve a rendszer regisztrálja az egyén íriszének mintázatát. Abban az esetben amikor egy személy beszkeneli a szemét, hogy például belépessen egy adott intézménybe, akkor a kamera összehasonlítja az adatbázisban levő

képeket, a beolvasott írisz mintával a döntéshozatal érdekében. A folyamat gyors, pár másodpercet igényel (Clodfelter, 2010).

Egyes fogyasztók véleménye szerint ezen megoldás, sokkal inkább tolatodóbbnak számít, az ujjlenyomat leolvasásához képest, míg a kínai felhasználók szerint sokkal higiénikusabb megoldást feltételez (Clodfelter, 2010).

2. **Melléklet** – Biometrikus fizetési megoldások előnyeinek és hátrányainak bemutatása

A biometrikus azonosítás és fizetés számos előnnyel rendelkezik (Mróz-Gorgoń et al., 2022; Kim et al., 2019). A legnagyobb előnyt a kimagasló biztonság és védelem jelenti a felhasználók számára (Clodfelter, 2010). A bankok minimalizálhatják a nem jogosult, hamis hozzáférést, autentifikációt (Liébana-Cabanillas et al., 2024), valamint abban az esetben, ha az ügyfél elveszíti vagy ellopják bankkártyáját, nem kell azzal a kockázattal szembesülnie, hogy egy nem kívánt személy felhasználja azt (Clodfelter, 2010). Ezen fizetési módszer, egy gyorsabb megoldást nyújt a vásárlóknak, körülbelül 70%-kal felgyorsíthatja a pénztárnál történő fizetést (Kumar & Ryu, 2009).

Egy további előny a kényelem, ugyanis a fogyasztónak nem szükséges magával vinnie pénztárcáját, a különböző bankkártyáit vagy mobiltelefonját (Kim et al., 2019), valamint nem szükséges a jelszavak észbetartása (Zarco et al., 2024). A költségmegtakarítás is egy előnyt jelenthet, ugyanis a fokozott biztonság miatt, a csalási arány is alacsonyabb lehet, ezáltal a visszaigénylések száma is csökkenhet. A feldolgozási és tranzakciós díjak is egyes esetekben alacsonyabbak, a hitelkártyákkal szemben (nttdatipay.com, 2024). Emellett a környezetvédelem is az előnyök közé sorolható, ugyanis a legtöbb biometrikus fizetési megoldások esetében, nem szükséges a bankkártyák gyártása, így nem kerül felhasználára műanyag, amely nagymértékben csökkentheti a környezetszennyezést (Kim et al., 2019).

Az előbbieken említett előnyök mellett, ezen technológia különböző hátrányokat is feltételez (Kim et al., 2019). Annak ellenére, hogy a biometrikus azonosítás magas biztonsági szintet és védelmet nyújt, ezen technológia mégsem jelent egy tökéletes megoldást (Kodituwakku, 2015). Bár ritka az előfordálása, de egyes esetekben megtörténhet, hogy hamis elfogadás történik a rendszer részéről. Összkeverednek az egyének biometrikus adatai ikrek vagy hasonló személyek esetében, ha az adatbázisban nem megfelelően voltak rögzítve az adatok vagy abban az esetben, ha a biometrikus szenzor nem megfelelően volt kalibrálva. Ezen hiba fordítottja is megtörténhet, amikor a beolvasó elutasít egy legitim személyt. Téves

elutasítás megtörténhet abban az esetben, ha például a kép elmosódik vagy az egyén egyes jellemzői megváltoznak, például arcfelismerés esetében, a személy megjelenése változik súlygyarapodás vagy fogyás során. Egyes kultúrákhoz tartozó személyek esetében a hamis elfogadás magasabb, fontos, hogy ezen rendszerek inkluzívak legyenek, ne merüljön fel kulturális vagy demográfiai diszkrimináció (Othman, 2024).

Egyes személyek számára, a biometrikus technológián alapuló rendszerek használata kényelmetlen lehet, kulturális okok, valamint vallási okok miatt (Clodfelter, 2010).

Egy további hátrány, az adatvédelmi aggályokat feltételezi, a felhasználók kockázatot érzékelnek az adataikkal szemben, tartanak attól, hogy a rögzített és tárolt adatokat feltörhetik és nem kívánt célokból, más személyek is felhasználhatják (Kim et al., 2019). Bár a biometrikus technológia általánosan véve biztonságosabb és nehezebben feltörhető, mint a jelszavak és a PIN kódok, vannak helyzetek amikor, például arcfelismerő rendszerek esetében, fényképek segítségével megtévesztik a rendszert és hozzáférnek az adott személy pénzügyeihez és adataihoz (Liébana-Cabanillas et al., 2024). Egy másik hátrány abból adódik, hogy ellentétben a hagyományos fizetési rendszerekkel, ahol a jelszó vagy a PIN kód módosítható, a biometrikus adatok nem módosíthatóak (Zarco et al., 2024).

Emellett hátrányt jelenthet az infrastruktúra kialakítása, ahhoz hogy ezen fizetési megoldás használható legyen, szükséges speciális szenzorok és rendszerek beszerelése a kereskedelmi egységekbe (Kim et al., 2019).