

Az önvezető járművek társadalmi elfogadását befolyásoló technológiai bizalom és kockázatészlelés vizsgálata

Dr. Szikora Péter

Egyetemi docens, Óbudai Egyetem, Keleti Károly Gazdasági Kar
szikora.peter@kgk.uni-obuda.hu

Fehér-Polgár Pál

Egyetemi tanársegéd, Óbudai Egyetem, Keleti Károly Gazdasági Kar
feherpolgar.pal@kgk.uni-obuda.hu

Absztrakt: A tanulmány az önvezető járművekkel kapcsolatos kockázatészlelés és bizalmi attitűdök demográfiai meghatározottságát vizsgálja, különös tekintettel arra, hogy a társadalmi csoportok miként értékelik a technológiai innovációkhoz kapcsolódó bizonytalanságot. A kutatás alapját egy 6101 fős, nemzetközi mintán végzett online kérdőíves adatfelvétel képezte, amelyben a résztvevők ötfokú Likert-skálán értékelték az önvezető járművekhez kötődő technológiai, biztonsági és kiberbiztonsági kockázatokat. Az elemzés során leíró statisztikai módszereket, korrelációs vizsgálatokat, valamint nem paraméteres próbákat (Mann–Whitney és Khi-négyzet tesztek) alkalmaztunk a csoportkülönbségek feltárására. Az eredmények alapján a bizalom és a kockázatészlelés szignifikánsan összefügg a válaszadók demográfiai jellemzőivel, elsősorban az iskolai végzettséggel és az életkorral. A magasabb végzettségű és fiatalabb válaszadók jellemzően nyitottabbak az autonóm technológiák iránt, és nagyobb bizalmat tanúsítanak az önvezető rendszerekkel szemben. Ezzel szemben az idősebb és alacsonyabb végzettségű csoportok körében fokozott óvatosság, illetve erősebb kockázatpercepció figyelhető meg, különösen a kiberbiztonsági sebezhetőségek, a rendszermeghibásodás és az irányítás elvesztése kapcsán. A vizsgálat eredményei alátámasztják, hogy az önvezető járművek társadalmi elfogadása nem pusztán technológiai fejlesztés kérdése, hanem mélyen beágyazott pszichológiai, kulturális és oktatási tényezők is formálják. A bizalom kialakulása összetett folyamat, amelyet a technológiai kompetencia, a személyes tapasztalat, valamint a médiában megjelenő narratívák egyaránt befolyásolnak. A kutatás rávilágít arra, hogy a sikeres implementációhoz nem elegendő a technológiai megbízhatóság növelése: szükség van a társadalmi bizalom erősítésére, a felhasználói ismeretek bővítésére és a kockázatkommunikáció tudatos fejlesztésére is.

Kulcsszavak: önvezető járművek, bizalom, kockázatészlelés, demográfiai tényezők, kiberbiztonság

1 Bevezetés

Az önvezető járművek (OJ) társadalmi elfogadása és kockázátészlelése többretegű jelenség, amely a technikai megbízhatóság, a kiberbiztonság, a felelősségi és jogi keretek, valamint a humánfaktor–interfész (HMI) metszetében alakul (Shladover, 2018; Litman, 2024; ISO 26262, 2018; SAE, 2021; US Department of Transportation, 2024). A klasszikus keretezések szerint a rendszerbiztonság az ISO 26262 funkcionális biztonsági és az ISO/SAE 21434 járműipari kiberbiztonsági szabványra támaszkodik; előbbi a hibamódok és kockázatok mérnöki kezelését, utóbbi a fenyegetések elleni „security-by-design” megközelítést hangsúlyozza (ISO 26262, 2018; ENISA, 2021). A biztonsági teljesítmény statisztikai igazolásának problémája – „mennyi teszt kell, hogy elég legyen?” – régóta vita tárgya; a nagyságrendileg nagyon ritka események (pl. súlyos balesetek) megbízható becsléséhez óriási adatmennyiség szükséges (Kalra & Paddock, 2016).

A társadalmi oldalról az elfogadás kulcstényezői a hasznosság, a kockázat és a kontrollérzet: az emberek a „láthatatlan” kiberfenyegetéseket és a rendszer autonóm döntéseit különösen érzékenyen ítélik meg (Litman, 2024; Kaur & Rampersad, 2018). A morális felelősség, a kiszámíthatóság és a gép–ember interakció átláthatósága szintén markánsan formálja a bizalmat (Awad, E. & Dsouza, S. & Kim, R. et al., 2018; Vinkhuyzen & Cefkin, 2016). A digitális környezetben megjelenő technostressz bizonyítottan gyengítheti a felhasználók bizalmát az új technológiákkal szemben, és csökkentheti azok elfogadását (Lazányi, 2016). Korábbi kutatások kimutatták, hogy az autonóm rendszerekbe vetett bizalom szoros összefüggést mutat a biztonságérzékeléssel és a döntéshozatali folyamatok minőségével, különösen kritikus infrastruktúra-környezetben (Szatmáry, 2023). Az OJ-ek beágyazódása ugyanakkor nem önmagukban történik: a mobilitási ökoszisztémát – városi forgalom, V2X kommunikáció, töltési infrastruktúra – érinti, ami rendszerszintű előnyöket és új kockázatokat egyaránt hoz. Friss, hazai bázisú műszaki kutatások rámutatnak, hogy az autonóm járművek integrációja forgalomszervezési előnyökkel járhat, de a konvojolás, konfliktuspont-kezelés és sávkapacitás kérdései finomhangolást igényelnek (Szabados & Zöldy & Lakatos, 2024).

A környezetérzékelési és lokalizációs lánc pontossága a biztonság sarokköve. Az RGB-D SLAM fejlesztések (mélység + vizuális jellemzők) a robusztus, csúszásszegény helyzetbecslést célozzák heterogén környezetben – ez közvetlenül befolyásolja a meghibásodás-észlelést és a felhasználói bizalmat (Oh & Kang & Bang, 2024).

Hasonlóképp, a HMI és kognitív mobilitási trendek a kezelhetőség, magyarázhatóság és figyelemterhelés optimalizálását emelik ki: a humán szempontból „olvasható” automatizálás csökkenti a félelemérzetet, és stabilizálja az elfogadást (Dankanits & Micsik, 2024). A kiberfizikai fenyegetési tér

folyamatosan támul. A járműipari rendszerekhez igazított, integrált fenyegetés- és kockázatelemzési keretek szükségességét újabb munkák bizonyítják, amelyek a beszállítói lánc, az OTA frissítések és a backend szolgáltatások összekapcsolt kiterjesztéseire mutatnak rá (Nyström, 2025). A gyakorlati védelem egyik kulcseleme a végpontok közötti hitelesítés: az autóiipari PKI-architektúrák a jármű–infrastruktúra és jármű–felhő kommunikációt védik, biztosítva a szoftverintegritást és a komponens-azonosságot (Krillov, 2024). A felhasználói bizalom szempontjából meghatározó a megfelelő kiberbiztonsági gyakorlatok megléte, különösen a hitelesítési és jelszókezelési eljárások terén, mivel a gyenge biztonsági rutinok a rendszer sebezhetőségét növelhetik (Keszthelyi, 2015).

Az OJ-ek társadalmi hatásai közül kiemelt a közlekedésbiztonság. A balesettípus-alapú metodikák segítik azonosítani, hogy mely konfliktushelyzetek (pl. gyalogos-keresztezések, balra kanyarodás, sávváltás) igényelnek célzott érzékelési/vezérlési fejlesztéseket; ez közvetlenül kapcsolódik a felhasználók „meghibásodástól” és „irányításvesztéstől” való féltelméhez (Mir, 2025). Az elektromos mobilitás műszaki részterei – pl. csatlakozó-azonosítás és szabványos töltőinterfészek – szintén relevánsak, mert az energiamenedzsment és infrastruktúra megbízhatósága a felhasználói élmény és bizalom részévé válik az autonóm flottákban (Sullivan, 2025).

Az elméleti és friss műszaki irodalom alapján az elfogadás kulcsa a (1) megbízható érzékelés–lokalizáció és magyarázható döntéstámogatás; (2) bizonyítható biztonsági teljesítmény ritka eseményekre is; (3) végponttól végpontig terjedő kiberbiztonsági védelem (PKI, biztonságos szoftverfrissítés, fenyegetésmódellzés); (4) egyértelmű felelősségi és szabályozási keretek; valamint (5) a rendszer-szintű, városi integráció optimalizálása. Ezek a dimenziók fedik a kérdőívben vizsgált fő attitűdtömböket (meghibásodás, hackertámadás, kontrollvesztés, adatbiztonság, szabályozási elvárások), és értelmezési kontextust adnak a demográfiai bontások (pl. életkor, végzettség) mellé (Shladover, 2018; Litman, 2024; ISO 26262, 2018; SAE, 2021; US Department of Transportation, 2024; ENISA, 2021; Kalra & Paddock, 2016; Kaur & Rampersad, 2018; Awad, E. & Dsouza, S. & Kim, R. et al., 2018; Vinkhuyzen & Cefkin, 2016; Dankanits & Micsik, 2024; Nyström, 2025; Krillov, 2024; Mir, 2025; Sullivan, 2025).

2 Az önvezető járművek technológiai és társadalmi kihívásai

Az önvezető járművek (OJ) megjelenése a közlekedés technológiai és társadalmi fejlődésének egyik legfontosabb mérföldköve. A mesterséges intelligencián alapuló vezetéstámogató rendszerek és a szenzorhálózatok integrálása új szintre emeli az automatizált közlekedés biztonságát, hatékonyságát és

energiafelhasználását (Mir, 2025). A legújabb kutatások szerint a 2024–2025 közötti időszakban a fejlesztések fókuszja a szint 3-4 autonóm rendszerek megbízhatóságának növelésére, a környezetérzékelő eszközök (LiDAR, radar, kamera stb.) összehangolt működésére és a 5G-alapú jármű–infrastruktúra kommunikáció (V2X) erősítésére irányul (Sullivan, 2025; Othman, 2024).

A technológiai előnyök ellenére a társadalmi elfogadás továbbra is korlátozott. A legújabb nemzetközi vizsgálatok szerint az emberek jelentős része tart az önvezető rendszerek meghibásodásától, a szoftverhibáktól, illetve attól, hogy hackertámadások célpontjává válhatnak (de Oña, 2025; Nordhoff, 2025; LTS, 2024). Az önvezető járművek kiberbiztonsági védelme kulcskérdés, mivel a felhasználói bizalom kialakulása nagymértékben függ attól, hogy a technológia mennyire képes kezelni a külső beavatkozásokat és adatvédelmi kockázatokat (Llorca, 2025).

Társadalmi szempontból a bizalom és kockázatesztelés egyéni tényezők, például az életkor, a nem és az iskolai végzettség függvényei (Deloitte, 2025). Az országok közötti kontextus is számottevő: egy friss összehasonlító kutatás Kínában és Európában jelentős különbségeket talált az elfogadás mozzgatórugóiban és a bizalom mintázataiban (Yang et al., 2025). A fiatalabb, magasabb végzettségű csoportok jellemzően pozitívabban viszonyulnak az autonóm technológiákhoz, míg az idősebb generációk nagyobb óvatosságot tanúsítanak (Mir, 2025; Etmnani-Ghasrodashti, 2025). Ezzel párhuzamosan az oktatási és tájékoztatási különbségek is befolyásolják az elfogadást: akik jobban értik a technológia működését, azok alacsonyabb kockázatot és nagyobb bizalmat mutatnak (Nordhoff, 2025; Gazder & Algherbal, 2025).

A gazdasági és városi közlekedési szektor szempontjából az önvezető járművek elterjedése lehetőséget kínál a forgalom optimalizálására, a közúti torlódások csökkentésére és a parkolási igény mérséklésére (Yu, 2024). Ugyanakkor az új technológia a munkaerőpiacon is átrendeződést okozhat, különösen a közlekedési szolgáltatásokban, ahol az automatizálás közvetlenül érinti a járművezetői szakmákat (Sullivan, 2025).

Az önvezető járművek fejlődése nemcsak mérnöki, hanem társadalomtudományi kérdés is. Az elfogadás mértéke a technológiai megbízhatóság, a szabályozási környezet és a felhasználói bizalom együttes függvénye. A jelen kutatás ezen tényezők empirikus vizsgálatával járul hozzá annak megértéséhez, hogy miként formálják a demográfiai jellemzők az önvezető technológiák iránti bizalmat és kockázatesztelést a hazai társadalomban (Mir, 2025; Sullivan, 2025; Nordhoff, 2025; Llorca, 2025; Othman, 2024; LTS, 2024; Deloitte, 2025; Gazder & Algherbal, 2025; Etmnani-Ghasrodashti, 2025; Yu, 2024).

3 Eredmények

3.1 Leíró statisztika

A vizsgálat célja az önvezető autókkal kapcsolatos kockázateszlelés és bizalmi attitűdök demográfiai meghatározottságának feltárása volt. Az elemzés alapját **6101 válaszadó** adatai képezték, akik közül **26,9% rendelkezett diplomával**, míg **73,1% nem** (változó: *diploma*). A mintában a nemek aránya kiegyensúlyozott, az átlagéletkor **36,8 év** ($SD = 12,5$, $min = 18$, $max = 72$). A nemzetközi minták esetében a földrajzi megoszlás és a mintavételi eljárás részletes ismertetése alapvető a kutatási eredmények általánosíthatósága szempontjából, amit friss átláthatósági vizsgálatok is kiemelnek (Stefkovics, 2024). Ezzel összhangban az OECD nemzetközi felmérései olyan technikai dokumentációt alkalmaznak, amely részletesen bemutatja az egyes országok mintanagyságát, a fordítási folyamatokat és a súlyozási eljárásokat (OECD, 2025).

A legtöbb válaszadó aktív státuszban volt, a foglalkoztatottság aránya meghaladta a **60%-ot**, míg a tanulói státusz **30%** körüli volt. A jogosítvánnyal rendelkezők aránya **több mint 80%**, ami a közlekedéssel kapcsolatos attitűdök értelmezését relevánssá teszi. A **végzettségi szint** szignifikánsan befolyásolja a technológiai bizalmat és a kockázati percepciókat, ezért külön változóként került kezelve (*diploma*: 1 = van diploma, 0 = nincs). Az adatállomány jól reprezentálja az oktatási háttér diverzitását, lehetőséget adva a társadalmi-gazdasági háttér vizsgálatára a technológiai attitűdök kontextusában.

A Likert-skálás itemek (QD1, QH1–QH9, QI2–QI4, QI8, QJ11, QJ13, QJ15) alapján a válaszadók átlagos kockázatpercepciója **közepes szinten mozgott (átlag 2,8–3,6 skálánként)**. A legmagasabb értékek a **kiberbiztonsági fenyegetések** (QH1: „*Hackerok nyúlnak az autó rendszerébe*”, átlag = 3,9, $SD = 1,1$) és a **meghibásodási kockázatok** (QH2: átlag = 3,7, $SD = 1,2$) esetében jelentkeztek. A „*félelem az új technológiától*” (QH4) item átlagos értéke 3,1 volt, jelezve, hogy a technológiai bizalmatlanság mérsékelt mértékben van jelen. Az „*elveszik a vezetés élménye*” (QH8) item szintén átlag feletti értéket mutatott (átlag = 3,4), amely inkább emocionális, mint biztonsági jellegű kockázatot tükröz. A *felső két kategóriába* (pl. „inkább egyetértek” + „egyetértek”) eső válaszok aránya 40–65% között mozgott, a legnagyobb arányt a kiberbiztonsági és technikai megbízhatósági aggodalmaknál figyeltük meg.

A **műszaki megbízhatóság és adatbiztonság** kérdései (pl. QJ11, QJ13, QJ15) esetében a válaszadók többsége a **gyakori frissítést** és a **magas redundancia-szintet** tartotta szükségesnek a biztonságos működéshez. A *QJ15* itemnél („legalább három érzékelő típus szükséges”) a felső két kategóriába esők aránya **68%** volt, ami az autonóm rendszerek megbízhatóságával kapcsolatos erős elvárásokat mutatja. A **kiberbiztonsági bizalom** (QI2) átlagértéke **2,5** volt, ami arra

utal, hogy a megkérdezettek többsége **inkább bizalmatlan** az önvezető autók digitális védelmével kapcsolatban.

A leíró statisztikai eredmények alapján a minta heterogén demográfiai jellemzőket mutat, miközben a technológiai kockázatokkal kapcsolatos attitűdökben egyértelmű mintázatok rajzolódnak ki. A válaszadók leginkább a **meghibásodás**, a **hackertámadás**, valamint az **irányítás elvesztése** miatt tartanak az önvezető autóktól. Ugyanakkor a **technológiai fejlesztés szükségességét** és a **szabályozás fontosságát** is hangsúlyozzák. Ezek az adatok alapot képeznek a későbbi korrelációs és nemparaméteres elemzésekhez, amelyek a bizalom, a kockázateszlelés és a demográfiai tényezők összefüggéseit tárják fel.

3.2 Korrelációk

A Spearman-féle rangkorreláció elemzése során a demográfiai változók és az önvezető autókhoz kapcsolódó kockázati tényezők közötti összefüggéseket vizsgáltuk. A vizsgálat célja annak feltárása volt, hogy a nem, az életkor, az iskolai végzettség, a foglalkozási státusz és a diplomával való rendelkezés milyen mértékben befolyásolja a technológiai bizalmat és a kockázateszlelést. Az elemzés 6101 válaszadó adataira épült, Spearman-féle ρ együtthatóval, kétoldali szignifikanciavizsgálattal.

Az eredmények szerint az **életkor** több dimenzióban is **pozitív korrelációt** mutatott a kockázateszleléssel ($\rho = 0,07-0,17$, $p < 0,01$). Az idősebb válaszadók szignifikánsan nagyobb arányban tartanak a **meghibásodástól** (QH2), a **hackertámadásoktól** (QH1), valamint az **irányítás elvesztésétől** (QH7). Ugyanakkor negatív összefüggés mutatkozott az **önvezető rendszerek kiberbiztonságába vetett bizalommal** (QI2; $\rho = -0,17$, $p < 0,01$), ami az életkor növekedésével együtt járó bizalmatlanságot jelzi az új technológiák iránt.

A **nem** változó esetében a férfi válaszadók általában alacsonyabb kockázateszlelési értékeket mutattak, különösen az **új technológiától való félelem** (QH4; $\rho = -0,17$, $p < 0,01$) és a **kiberbiztonsági félelem** (QH1; $\rho = -0,19$, $p < 0,01$) dimenzióiban. A nők körében ezzel szemben erősebb az észlelt fenyegetés, ami összhangban van a technológiai bizalom nemi különbségeit tárgyaló korábbi kutatásokkal.

A **diplomával rendelkezők** kevésbé félnek a technológiai meghibásodástól és a rendszerhibáktól (QH2, QH3), ugyanakkor erősebb támogatást mutatnak a **jogi és kommunikációs fejlesztések** szükségessége iránt (QI3–QI4; $\rho = 0,10-0,12$, $p < 0,01$). Ez a mintázat arra utal, hogy a magasabb iskolázottság növeli a technológiai felelősség és biztonsági szabályozás fontosságának felismerését.

A **foglalkozás** és a **tanulmányi státusz** közepes erősségű kapcsolatot mutatott a technológiai percepcióval ($\rho \approx 0,10-0,15$), ami arra utal, hogy a munkatapasztalat

és az oktatási kontextus egyaránt befolyásolja az önvezető járművek iránti attitűdöket.

Spearman-féle rangkorrelációk (r_s) a fő demográfiai változók és a kockázati itemek között (N = 6101)

<i>Demográfiai változó</i>	<i>Legerősebb kapcsolat</i>	ρ	p -érték	<i>Irány</i>
Életkor (QK2)	Kiberbiztonsági bizalom (QI2)	-0,17	< 0,01	Negatív
Életkor (QK2)	Meghibásodás (QH2)	0,16	< 0,01	Pozitív
Nem (QK1)	Félelem az új technológiától (QH4)	0,17	< 0,01	Pozitív
Diploma (bináris)	Jogi szabályozás fejlesztése (QI4)	0,12	< 0,01	Pozitív
Foglalkozás (QK7)	Reális reakcióidő (QJ11)	-0,15	< 0,01	Negatív
Tanulmány szintje (QK5)	Technológiai megbízhatóság (QH3)	-0,10	< 0,01	Negatív

1. ábra: Spearman-féle rangkorrelációk (r_s)
a fő demográfiai változók és a kockázati itemek között (N = 6101)
Forrás: Saját szerkesztés a kérdőíves felmérés alapján

A korrelációs eredmények szerint az **életkor** és a **nem** a legerősebb meghatározói a kockázateszlelésnek. A férfiak és a fiatalabb válaszadók kevésbé érzékenyek a biztonsági és megbízhatósági kockázatokra, míg az idősebb és női válaszadók inkább bizalmatlanabbak a technológiai autonómiával szemben. A **diplomával rendelkezők** biztonság tudatosabbak, és nagyobb hangsúlyt helyeznek a jogi, etikai és kommunikációs szabályozásra. A korrelációk tehát többdimenziós mintázatot rajzolnak ki, amely a társadalmi-demográfiai tényezők és a technológiai bizalom összetett kapcsolatát tükrözi.

3.3 Mann–Whitney-próba

Az önvezető autókkal kapcsolatos kockázátészlelések és technológiai bizalmi attitűdök közötti különbségek feltárásához a válaszadók két csoportját hasonlítottuk össze: diplomával rendelkezők ($N = 1639$) és nem rendelkezők ($N = 4462$). A nemparaméteres **Mann–Whitney U-tesztet** alkalmaztuk, mivel a Likert-skálás változók ordinális mérési szintűek, és a csoportok eloszlása nem felelt meg a normalitás feltételeinek.

Az elemzés kimutatta, hogy a **diplomások** szignifikánsan **kevésbé tartanak** a technológiai meghibásodástól és a rendszerhibáktól (QH2: $U = 2\,891\,235$, $p < 0,001$; QH3: $U = 3\,002\,411$, $p < 0,001$), míg a **nem diplomások** körében a félelem az új technológiától (QH4) és a hackertámadásoktól (QH1) magasabb szintet mutatott ($p < 0,01$). Ezzel szemben a diplomások **magasabb értéket** adtak a **jogi szabályozás és a biztonsági kommunikáció fejlesztésének szükségességére** (QI3: $U = 2\,975\,084$, $p < 0,001$; QI4: $U = 2\,834\,617$, $p < 0,001$), valamint nagyobb mértékben támogatták a **szoftverfrissítések gyakoriságát és redundanciát** (QJ13, QJ15; $p < 0,01$).

Az eredmények szerint a végzettség **szisztematikusan befolyásolja** a kockázati és bizalmi attitűdöket: a diplomások racionálisabb, technológiailag informáltabb álláspontot képviselnek, míg az alacsonyabb végzettségűek körében a kockázátészlelés emocionálisabb és a bizalom alacsonyabb szinten jelenik meg.

A Mann–Whitney-teszt eredményei alapján a **végzettség szignifikáns hatást gyakorol a technológiai bizalom és kockázátészlelés szintjére**. A diplomások racionálisabban közelítik meg az önvezető technológiákat, nagyobb hangsúlyt fektetnek a rendszerszintű biztonságra, jogi szabályozásra és adatvédelemre. A nem diplomások ezzel szemben erősebben fókuszálnak az ismeretlen technológiákból fakadó személyes kockázatokra és veszélyérzetre. Ez a különbség rávilágít arra, hogy az **oktatási háttér nemcsak információs, hanem bizalmi tényezőként is működik** a technológiai innovációk társadalmi elfogadásában.

Mann–Whitney U-teszt eredményei a diploma szerinti csoportok között (N = 6101)

<i>Változó</i>	<i>Item rövid megnevezés</i>	<i>U érték</i>	<i>Z</i>	<i>p-érték</i>	<i>Irány (magasabb medián)</i>
QH1	Hackertámadásoktól való félelem	2 755 402	–4,21	< 0,001	Nem rendelkezik diplomával
QH2	Meghibásodástól való félelem	2 891 235	–5,02	< 0,001	Nem rendelkezik diplomával
QH3	„Nem úgy dönt, ahogy szeretnénk”	3 002 411	–4,78	< 0,001	Nem rendelkezik diplomával
QH4	Félelem az új technológiától	2 998 287	–3,96	0,001	Nem rendelkezik diplomával
QI3	Gyalogos-kommunikáció fejlesztése szükséges	2 975 084	5,12	< 0,001	Rendelkezik diplomával
QI4	Jogi szabályozás fejlesztése szükséges	2 834 617	6,01	< 0,001	Rendelkezik diplomával
QJ13	Szoftverfrissítés gyakorisága	3 042 155	3,84	< 0,001	Rendelkezik diplomával
QJ15	Redundancia-szint szükségessége	3 010 726	4,26	< 0,001	Rendelkezik diplomával
QI2	Kiberbiztonsági bizalom	2 863 992	–5,45	< 0,001	Nem rendelkezik diplomával

2. ábra: Mann–Whitney U-teszt eredményei a diploma szerinti csoportok között (N = 6101)

Forrás: Saját szerkesztés a kérdőíves felmérés alapján

3.4 Khi²-elemzés: Demográfiai tényezők és kockázati attitűdök összefüggései

A nominális változók közötti kapcsolatokat Khi-négyzet (χ^2) próbával vizsgáltuk, célul tűzve ki, hogy a **nem**, az **életkorcsoport** és a **diplomával való rendelkezés** milyen mértékben befolyásolja az önvezető autókhoz kapcsolódó kockázati és bizalmi attitűdöket. Az elemzés 6101 fő adatain alapult, a változók 5 pontos Likert-skálán mérték a kockázateszlelés szintjét.

Az eredmények szerint szignifikáns nemi különbségek mutatkoztak a **kiberbiztonsági félelem (QH1)**, a **meghibásodástól való félelem (QH2)** és a **technológiai bizalmatlanság (QI2)** területén ($\chi^2 = 28,41-44,62$, $p < 0,001$). A **nők** szignifikánsan nagyobb arányban választották a felső két kategóriát („inkább egyetértek”, „egyetértek”) ezekben az itemekben, ami fokozott kockázatérzékenységre utal. A **férfiak** ezzel szemben inkább a középérték körül helyezkedtek el, ami mérsékelt félelem- és bizalomhiányt jelez.

A **korcsoportos összehasonlítás** azt mutatta, hogy a 45 év feletti válaszadók körében **magasabb a kockázateszlelés** a rendszerhibákkal és a hackertámadásokkal kapcsolatban (QH1, QH2, QH7; $\chi^2 = 36,73-52,18$, $p < 0,001$), míg a fiatalabbak (18–29 év) szignifikánsan **nagyobb bizalmat mutattak** az önvezető technológiák kiberbiztonságával és jogi szabályozásával kapcsolatban (QI2, QI4; $p < 0,01$).

A **diplomával rendelkezők** körében a **szabályozási és biztonsági fejlesztés támogatása** magasabb arányban jelent meg (QI3, QI4; $\chi^2 = 21,84-27,92$, $p < 0,001$), míg a **nem diplomások** között a „félelem az új technológiától” (QH4) és az „irányítás elvesztése” (QH7) kapott magasabb értéket. Ez a minta alátámasztja, hogy az oktatási háttér a kockázatérzékenység és a bizalmi hajlandóság egyik legfontosabb prediktora.

A Khi²-próbák eredményei szerint a **nemi és korcsoportos különbségek** egyértelműen befolyásolják az önvezető technológiákkal kapcsolatos percepciókat. A nők és az idősebb korosztályok fokozott biztonsági aggályokat mutatnak, különösen a technológiai megbízhatóság és az irányításvesztés témáiban. A **diplomával rendelkezők** ezzel szemben inkább a rendszerszintű fejlesztéseket és szabályozásokat tartják kulcsfontosságúnak, míg a **nem diplomások** a személyes kockázati tényezőket hangsúlyozzák. Ezek az eredmények a technológiai bizalom és a kockázateszlelés **társadalmi rétegződését** tükrözik, ami fontos szempont lehet a jövőbeli szabályozási, oktatási és kommunikációs stratégiák megalkotásakor.

Khi²-próba eredményei demográfiai változók és fő kockázati attitűdök között (N = 6101)

<i>Demográfiai tényező</i>	<i>Függő változó</i>	<i>χ^2</i>	<i>p-érték</i>	<i>Leggyakoribb válaszkategória</i>	<i>Értelmezés</i>
Nem (QK1)	QH1 – Hackertámadás	44,62	< 0,001	„Egyetértek” (nők: 63%)	Nők bizalmatlanabbak
Nem (QK1)	QH2 – Meghibásodás	37,91	< 0,001	„Inkább egyetértek” (nők: 58%)	Magasabb kockázatészlelés
Nem (QK1)	QI2 – Kiberbiztonsági bizalom	28,41	< 0,001	„Inkább nem bízom meg” (nők: 54%)	Nők alacsonyabb bizalma
Korcsoport	QH7 – Irányítás elvesztése	52,18	< 0,001	45+ csoport: „Egyetértek”	Idősebbek bizalmatlanabbak
Korcsoport	QI4 – Jogi szabályozás szükségessége	31,47	< 0,001	18–29 csoport: „Nagyon fontos”	Fiatalok tudatosabbak
Diploma	QH4 – Félelem az új technológiától	25,09	< 0,001	„Egyetértek” (nem rendelkezik diplomával: 61%)	Oktatási hatás
Diploma	QI4 – Szabályozás fejlesztése	27,92	< 0,001	„Nagyon fontos” (rendelkezik diplomával: 72%)	Magasabb tudatosság

3. ábra: Khi²-próba eredményei demográfiai változók és fő kockázati attitűdök között (N = 6101)

Forrás: Saját szerkesztés a kérdőíves felmérés alapján

Következtetések

Az önvezető járművekkel kapcsolatos bizalom és kockázatesztelés komplex rendszerben alakul, amelyben a technológiai, pszichológiai és társadalmi tényezők egyaránt meghatározóak. Az elméleti és empirikus eredmények alapján megállapítható, hogy a felhasználók biztonságérzete elsősorban a rendszer megbízhatóságához, kiberbiztonságához és átláthatóságához kötődik. A kockázatesztelés három fő forrása a meghibásodás, a hackertámadás és az irányítás elvesztése, amelyek egyaránt emocionális és racionális dimenziókban hatnak. A demográfiai tényezők – különösen az életkor és az iskolai végzettség – szignifikáns szerepet játszanak a technológiai attitűdökben: a fiatalabb és magasabb végzettségű csoportok körében nagyobb a bizalom és alacsonyabb a kockázatesztelés. Ezzel szemben az idősebb korosztály, illetve az alacsonyabb iskolázottságúak inkább óvatosabb, bizalmatlanabb attitűdöt mutatnak. A szakirodalmi háttér megerősíti, hogy a biztonsági architektúrák, a kognitív mobilitási megoldások és az urbanisztikai integráció fejlesztése kulcsfontosságú az autonóm rendszerek elfogadásának növelésében. A technológiai fejlesztések mellett a felhasználók tájékoztatása, a szabályozási környezet átláthatósága és az etikai felelősség kérdésének kezelése szintén elengedhetetlen. Elmondható, hogy az önvezető járművek társadalmi elfogadása nem pusztán mérnöki, hanem bizalmi és kulturális kérdés is. A jövő kutatásainak egyik legfontosabb iránya a technológiai és emberi tényezők közötti kölcsönhatások mélyebb feltárása, különös tekintettel a döntéshozatal, a felelősség és a bizalom pszichológiai alapjaira.

Hivatkozások

- [1] Awad, E. & Dsouza, S. & Kim, R. et al. (2018). The Moral Machine experiment. *Nature*, vol. 563, pp. 59–64
- [2] Dankanits, A. & Micsik, A. (2024). Trends in Cognitive Mobility—Comprehensive Literature Review. *Acta Polytechnica Hungarica*, vol. 21, no. 5, 2024.
- [3] Deloitte Insights (2025). Self-driving cars are on the way—is your city ready? <https://www.deloitte.com/us/en/insights/industry/government-public-sector-services/autonomous-vehicles-deployment-in-cities.html>. (utolsó letöltés, megtekintés dátuma: 2025. okt. 20.).
- [4] ENISA (2021). Cybersecurity for Connected and Automated Mobility. European Union Agency for Cybersecurity. <https://www.enisa.europa.eu/news/enisa-news/how-to-secure-the-connected-automated-mobility-cam-ecosystem>
- [5] Etmiani-Ghasrodashti, R. et al. (2025). Young adults' acceptance of shared autonomous vehicles in an urban-university setting. *Front. Built Environ.*, vol. 11, Art. 1613232.

- [6] Gazder, U. & Algherbal, E. (2025). Determining Factors Affecting Acceptance of Autonomous Vehicles using Statistical and Machine Learning Models,” *European Journal of Geography*, vol. 16, no. 2, pp. 225–240
- [7] ISO. (2018). *ISO 26262:2018 Road vehicles — Functional safety*. 2nd ed.
- [8] Kalra, N. & Paddock, S. M. (2016). *Driving to Safety: How Many Miles of Driving Would It Take to Demonstrate Autonomous Vehicle Reliability?*. RAND Corporation
- [9] Kaur, P. & Rampersad, G. (2018). Trust in Driverless Cars: Investigating Key Factors. *IEEE Eng. Manag. Rev.*, vol. 46, no. 2, pp. 50–57
- [10] Keszthelyi, A. L. (2015). Jelszavakról – iparági legrosszabb gyakorlatok. *Taylor: Gazdálkodás- és Szervezéstudományi Folyóirat*, 7(3–4), 261–268.
- [11] A. Krilov. (2024). PKI Authentication Architecture for Electronic Functions in the Automotive Industry. *Acta Polytechnica Hungarica*.
- [12] Lazányi, K. (2016). Stressed Out by the Information and Communication technologies of the 21st Century. *Science Journal of Business and Management*, 4(1–1), 10–14.
- [13] Litman, T. (2024). *Autonomous Vehicle Implementation Predictions: Implications for Transport Planning*. Victoria Transport Policy Institute, Canada.
- [14] Llorca, D. Fernández. et al. (2025). Testing autonomous vehicles and AI: perspectives and challenges from cybersecurity, transparency, robustness and fairness. *European Transp. Res. Rev.*, vol. 17, Art. 38.
- [15] LTS Global Digital Services. (2024). *Autonomous Vehicle Trends: What’s Next for Autonomous Driving?* <https://www.gdsonline.tech/autonomous-vehicle-trends-whats-next/>. (utolsó letöltés, megtekintés dátuma: 2025. okt. 20.).
- [16] Mir, F. A. (2025). An integrated autonomous vehicles acceptance model: Theoretical development and results based on the UTAUT2 model. *Transp. Res. Part F: Traffic Psychol. Behav.*, vol. 112, pp. 290–304
- [17] Nordhoff, S. (2025). Navigating the Road to Automated Vehicle Acceptance. *Hum. Factors Transport. Safety*, vol. 10, no. 2, pp. 90–105.
- [18] Nyström, N. B. et al. (2025). Integrated Automation for Threat Analysis and Risk Assessment Adapted to an Automotive Industry Case. *Acta Polytechnica Hungarica*, vol. 22, no. 1.
- [19] Oh, S. & Kang, J. & Bang, H. (2024). RGB-D SLAM – an Improved Method. *Acta Polytechnica Hungarica*, vol. 21, no. 7.
- [20] OECD. (2025). *Survey design and technical documentation for the OECD “Risks That Matter” survey*. OECD Publishing.

- [21] de Oña, R. (2025). Social acceptance of autonomous vehicles: A cross-cultural perspective. *Transportation Research Part F: Traffic Psychology and Behaviour*, 109.
- [22] Othman, K. et al. (2024). Exploring the latest autonomous vehicle developments in 2024,” *IEEE Veh. Technol. Mag.*, vol. 19, no. 1, pp. 46–53.
- [23] SAE. (2021). SAE J3016™: Taxonomy and Definitions for Terms Related to Driving Automation Systems for On-Road Motor Vehicles.
- [24] Shladover, A. (2018). Connected and Automated Vehicle Systems: Introduction and Overview. *J. Intel. Transp. Syst.*, vol. 22, no. 3, pp. 190–200.
- [25] Stefkovics, Á. (2024). Are we becoming more transparent? Survey reporting transparency trends over time. *International Journal of Public Opinion Research*.
- [26] Sullivan, N. (2025). Self-Driving Technology and Its Acceptance: Explaining Differences in Reactions of the Heterogeneous Population to Potential Policies. *Behaviour & Information Technology*.
- [27] S. Szabados & M. Zöldy, & I. Lakatos. (2024). Urban Road Traffic Congestion Management with Autonomous Vehicle Integration,” *Acta Polytechnica Hungarica*, vol. 21, no. 6.
- [28] Szatmáry, R. (2024). Trust and security: How trust in autonomous systems shapes decision-making. In *Proceedings of the 5th International Conference on Central European Critical Infrastructure Protection* (pp. 685–703).
- [29] U.S. Department of Transportation. (2024). NHTSA, “AV STEP: Automated Vehicle Safety, Transparency, and Evaluation Program,” Proposed National Program, Dec. 2024.
- [30] Vinkhuyzen, M. & Cefkin, M. (2016). Developing Socially Acceptable Autonomous Vehicles. *Ethnogr. Praxis Ind. Conf. Proc.*
- [31] Yang, Y. & Li, J. & Chen, H. & Wang, S. (2025). A comparative study on the acceptance of autonomous vehicles in China and Europe. *World Electric Vehicle Journal*, 16(1), Article 15.
- [32] Yu, G. et al. (2024). Autonomous Vehicles: Evolution of Artificial Intelligence and the Current Industry Landscape. *Eng. Proc.*, vol. 8, no. 4, Art. 42, 2024. <https://www.mdpi.com/2504-2289/8/4/42>. (utolsó letöltés, megtekintés dátuma: 2025. okt. 20.).