ÓBUDAI EGYETEM
ÓBUDA UNIVERSITY

DOKTORI (PHD) ÉRTEKEZÉS TERVEZET

HEGYI HENRIETTA

Internetkapcsolatra képes személygépjárművek információs rendszereinek biztonsági vizsgálata

Témavezető: dr.Erdődi László

BIZTONSÁGTUDOMÁNYI DOKTORI ISKOLA

Budapest, 2024.12.16.

TARTALOMJEGYZÉK

1. BEVEZETÉS

Napjaink személygépjárműveinek szolgáltatásai gyakran olyan folyamatokat kapcsolnak össze, amelyek az adatok feldolgozását szabályozzák, de ezek a folyamatok sokszor lazán meghatározottak és/vagy nem teljesen összeegyeztethetők, például a kért szolgáltatások nyújtása, a biztonságos használat, a viselkedésértékelés, valamint az üzleti tevékenységek működtetése és bővítése terén. [1] Az eredetileg karbantartási vagy felhasználói élmény fokozásának céljával [2] gyűjtött adatokat az érintettek beleegyező nyilatkozata esetén a biztosítótársaságok felhasználhatják a járművezetői profilok gazdagítására, egyéni árazási módok, akciók kialakítására, a vezetési magatartáson alapuló biztosítási kötvények kínálásához vagy az autóbalesetekben fennálló felelősség kivizsgálására. [3] A főként az ipar 4.0 technológiákat érintő komplexitásból fakadó szabályozási problémákra a COVID-19 időszaka is rámutatott. [4], [5]. Megfelelő szabályozási környezetben a közlekedésbiztonsági hatóságok is felhasználhatják ezeket az adatokat a közlekedési szabályok betartatására, például a sebességkorlátozások ellenőrzésére. A személyautóhasználatára vonatkozó minden egyes adat, például a vezetési útvonalak és úticélok, az autóba épített kommunikációhoz szükséges adatok vagy az infotainment-szolgáltatások használata során keletkező adatok érzékeny információkat tárhatnak fel az adott személy életéről. Az emberek vezetési rutinja és az érdeklődési körükbe tartozó helyek nemcsak az azonosításukat teszik lehetővé [6], hanem – például az általuk látogatott helyszínek ismeretében – olyan jellemvonásokra is következtethet az adatfeldolgozó, mint a vallás, politikai kötődés, a szexuális irányultság és az egyéb emberi kapcsolatok. Ezért az összegyűjtött adatok hasznosak az egyének profilalkotásához és megfigyeléséhez, különösen akkor, ha a személyes adatok meglévő (magán- vagy kormányzati) adatbázisaihoz kapcsolódnak vagy például a mobiltelefonjaik által gyűjtött adatokkal kapcsolják össze azokat (amelyen gyakran a járműhöz tartozó applikáció és annak adatai is megjelennek). [7]

Ezen információk érzékeny jellege miatt szükség lenne az adatvédelmi és információbiztonsági alapelvek alapos alkalmazására, különösen a célhoz kötöttség, az adatok minimalizálása és az adatok tárolása tekintetében. Mivel azonban az adatáramlás nem átlátható, a személygépjárművet vezető emberek többsége pedig nem kap tájékoztatást erre vonatkozóan – sőt, egyes esetekben nem is tud róla, hogy az adatai kikerülnék a járműből – így egyelőre nem jelenik meg olyan erős igény a piacon, ami segítené ezt a folyamatot. Míg a jövő önvezető autói és a közlekedési infrastruktúrával

kommunikálni képes járművek világában mindenki egyetért azzal kapcsolatban, hogy az adatok biztonsága kulcsfontosságú, a jelenünkben egy olyan világban élünk, ahol az emberek az okostelefonokhoz hasonló információgyűjtő készülékekben utaznak, mit sem sejtve ennek veszélyeiről.

Bár a különböző autóiparban alkalmazott szabványok és jogszabályok ma már magukba foglalják az ellátási lánc védelmét is, amely sok esetben a beszállítóknak a gyártóval egyenértékű szintű szabványoknak való megfelelését jelenti, sajnos legtöbb esetben csak egy keretet határoznak meg és nem adnak konkrét utasításokat a végrehajtással kapcsolatban. Ez bizonyos mértékben szükséges is, hiszen a különböző speciális helyzetek miatt adott fokú rugalmasság kulcsfontosságú. Alkalmazásuk azonban még így is esetleges, egységesen kötelező egyenszilárd kiberbiztonsági követelményrendszerről nem beszélhetünk, így a szándék ellenére csak ritka esetekben valósul meg, hogy a teljes termékéletciklusra vonatkozóan alkalmazásra kerüljön egy adott módszertan, vagy lefedje azt egy információbiztonsági irányítási rendszer.

Mint minden egyéb szervezetirányítási területen, a mérőszámok információbiztonsági szempontból is fontos szerepet játszanak, mivel ezek hiányában nem tudjuk mérni a biztonsági politika, mechanizmusok vagy megvalósítások sikerét. A különböző kockázatelemzési módszerek emiatt hatékony eszközt jelenthetnek az információbiztonsági szakemberek számára, hogy mérjék a rendszerek, termékek, folyamatok biztonsági szintjét, valamint a biztonsági problémák kezelésére való felkészültségüket. A mérőszámok segíthetnek a rendszer sebezhetőségének azonosításában is, útmutatást nyújtva a korrekciós prioritások meghatározásához.

1.1 A tudományos probléma megfogalmazás

A személygépjárműipar, ahogyan más iparágak is, akkor képes versenyképes maradni és megfelelő termékeket gyártani, ha a különböző mérnöki területek, a gépészeti, villamosmérnöki és informatikai szaktudás gördülékenyen képes együttműködni, kiegészíteni egymást. [8] Mivel azonban az informatika napjainkban az egyik leggyorsabban fejlődő tudományág, mely nagy mértékben specializálódik, ezért ezt a szinergiát egyre nagyobb kihívás megtartani. A klasszikus mérnöki területekre jellemző szigorú és következetes követelmények az informatikai kompetenciák és modern informatikai eszközök tekintetében még mindig kialakulóban vannak és több olyan területre is jellemző, hogy nem léteznek vagy csak csekély területet fednek le a kötelező

érvényű egzakt szabályozások, amelyek már régóta használatban vannak. Ilyenek például az adatfeldolgozási rendszerek, a gépi tanulási rendszerek vagy az IoT (Internet of Things) eszközök.

Az "internetkapcsolatra képes személygépjármű" vagy connected car fogalmát többféleképpen definiálják, de általánosságban olyan járművek tartoznak ide, amelyek képesek adatokat gyűjteni és megosztani a gyártóval (OEM - Original Equipment Manufacturer) vagy harmadik felekkel, mint például biztosítótársaságok, szervizek, városi infrastruktúra, vagy akár felhő alapú szolgáltatásokkal. Az internetkapcsolat lehetővé teszi, hogy ezek a járművek az utasok biztonságának növelése érdekében helyadatokat, járműállapot-információkat és más adatokat továbbítsanak, amelyeket többnyire SIM-kártyán vagy beépített kommunikációs eszközökön keresztül továbbítanak a megfelelő platformokra [9], [10].

A connected car, vagy magyarul internetkapcsolatra képes jármű fogalmát a tudományos irodalom több aspektusból tárgyalja, különös figyelmet szentelve a járművek kommunikációs képességeire és adatmegosztási lehetőségeire. Az internetkapcsolatra képes járművek általában olyan gépjárművek, amelyek képesek adatokat küldeni és fogadni, kapcsolódva más eszközökhöz vagy rendszerekhez – ez magában foglalhatja a gyártók szervereit, más járműveket, infrastruktúrát, vagy akár felhőalapú szolgáltatásokat is.

A Sensors folyóirat egyik cikke kiemeli a connected car technológia szerepét az adatgyűjtés és a közlekedés hatékonyságának növelése kapcsán. Ebben a tanulmányban a connected car vagy connected vehicle névvel illetett rendszereket olyan járművekként határozzák meg, amelyek támogatják a különböző vezetéstámogató alkalmazásokat, valós idejű navigációt, illetve a forgalomfigyelő szolgáltatásokat (pl. útvonaloptimalizálás). A járművek így a nagyobb biztonság és hatékonyság elérésében is szerepet játszanak, összekapcsolva őket a környezetükkel, illetve más járművekkel és rendszerekkel [11].

Az IEEE *„Intelligent and Connected Vehicles”* cikkében a szerzők továbbá megkülönböztetik az önálló internetkapcsolattal rendelkező járműveket és az okostelefonon keresztül internethez kapcsolódó járműveket. Az önálló kapcsolattal bíró járművek beépített SIM-kártya vagy Wi-Fi segítségével kapcsolódnak az internethez, míg a másik típus a mobilalkalmazás által biztosított adatkapcsolatra támaszkodik – tehát egy

rosszindulatú szereplő által alapvetően csak fizikailag, a járművet megközelítve vagy pedig a mobilalkalmazáshoz való jogosulatlan hozzáférés révén érhetőek el az adatok. Ez az utóbbi megoldás – bár biztonságosabbnak hangzik – nem olyan elterjedt, gyakran kiegészítő interfészként működik, például Bluetooth vagy Wi-Fi kapcsolaton keresztül .[12] A jelenlegi technológiai trendek alapján tehát az összekapcsolt járművek két fő adatkapcsolati típussal rendelkezhetnek:

Közvetlen internetkapcsolat	**Mobilalkalmazás-alapú adatkapcsolat**
A jármű önállóan, beépített SIM-kártya vagy Wi-Fi segítségével csatlakozik az internethez. Ezek a járművek a gyártók szervereire, valamint harmadik felek részére (pl. köztes adatfeldolgozó központok biztosítókhoz) továbbíthatnak adatokat. A legtöbb modern, közvetlen internetkapcsolattal ellátott jármű már rendelkezik különböző szenzorokkal és rendszerekkel, amelyek a jármű technikai állapotát vagy éppenséggel a sofőr viselkedését elemzik. [13]	Ezekben az esetekben a jármű nem rendelkezik saját, önálló adatkapcsolattal, hanem az okostelefon alkalmazásán keresztül továbbít adatokat. A mobilappok Bluetooth vagy Wi-Fi segítségével kapcsolódnak a járműhöz, majd a telefon internetkapcsolatán keresztül küldenek adatokat a gyártóhoz vagy egyéb rendszerekhez. Ez a típus gyakran a felhasználó aktív részvételét igényli, például külön bejelentkezés vagy az app megnyitása által [14], [15].

1. táblázat - Az internethez csatlakozó személygépjárművek két típusa a csatlakozás módja szerint

Az összekapcsolt jármű rendszere adatvédelmi szempontból egyértelműen a GDPR szabályozás hatálya alá esik, azonban egy ilyen komplex termék esetén nehezen meghatározható a vizsgálat tárgya (pl. az egész jármű, egyes elemek, szoftverek, hardverek) és a felelősség is (gyártó, fejlesztő, összeszerelő). Szerencsére a jogszabályok világszerte egyre nagyobb hangsúlyt helyeznek a *„privacy by design”* megközelítésre, azaz a járművek tervezésénél előzetesen figyelembe kell venni az adatvédelem szempontjait.[16]

A téma aktualitását fokozza az a trend, hogy az Európai Unióban a személygépjárműtervezés és gyártás piacán egyre hangsúlyosabban jelennek meg a harmadik országbeli gyártók, azon belül is a Kínai Népköztársaságból érkező személygépkjárművek. Mivel ez egy viszonylag új folyamat, az Európai Uniónak szemléletmódváltásra van szüksége a szabályozásainak megfelelő frissítéséhez, új

szabályzati környezet kialakításához. Az információbiztonsági szabványok, jogszabályok és ajánlások célja gyakran annak megjelölésére korlátozódik, hogy *minek* kell megfelelnie az azt alkalmazó szervezetnek. A *hogyan* kérdésre éppen ezért ezek a dokumentumok, rendszerek nem adnak egyértelmű válaszokat, azokat a szervezet maga, illetve a felkészítést végző munkavállalók vagy szervezeten kívüli tanácsadók határozzák meg és indokolják meg az auditon.[17] Ez a rugalmasság egyrészt lehetővé teszi, hogy a különböző profilú, méretű és más-más adottságokkal rendelkező vállalatok a saját, bevált módszereiket alkalmazhassák egy külső, kényszerűségből bevezetett megszabott módszertan helyett, másrészt viszont emiatt nehéz egy olyan stabil, egyenszilárd eredményt elérni általuk, aminek köszönhetően minden vállalat egyforma mélységben és részletességben alkalmazza őket. Ezzel együtt ez a szemléletmód magában hordozza a veszélyt, hogy az auditalany szempontjából kevésbé jól kezelt folyamatok kisebb hangsúlyt kapnak, illetve a szándékos félrevezetés előtt is megnyitja a kapukat.

A múltban több olyan esemény is történt, mely jól szemlélteti a problémát mind a szabályozási környezet, mind a szemléletbeli hiányosságok, mind pedig a helyzet komplexitása tekintetében:

A General Motors részéről például több mint öt évet vett igénybe, hogy kijavítson egy súlyos sérülékenységet az OnStar rendszerében, amely lehetővé tette a hackerek számára, hogy távolról átvegyék az irányítást a járművek felett. A probléma már 2010-ben ismertté vált, de a teljes megoldást csak 2015-ben vezették be. A sebezhetőség révén a támadók akár a fékrendszert is manipulálhatták. Azóta a GM megerősítette a kiberbiztonsági rendszerét, és gyorsabb válaszidőt biztosít a hasonló problémákra, felismerve a járművek digitalizációjával járó kockázatokat. [18]

A 2015-ös Jeep Cherokee hack egy mérföldkő volt az autóipari kiberbiztonság terén. Két kutató, Charlie Miller és Chris Valasek, távolról képes volt leállítani a jármű motorját és irányítani kritikus funkciókat, miközben az egy újságíróval a fedélzeten az autópályán haladt. A demonstráció rávilágított arra, hogy az internethez kapcsolt járművek sérülékenyek a távoli támadásokkal szemben. Az eset nyomán a Chrysler 1,4 millió járművet hívott vissza biztonsági frissítésre. Ez az incidens figyelmeztetésül szolgált az autóipar számára a digitális biztonság prioritásának szükségességéről. [19]

Sam Curry biztonsági kutató egyik blogbejegyzése egy olyan súlyos sebezhetőségről számol be, amely révén a hackerek képesek lehettek Kia járműveket távolról vezérelni.

A támadók mindössze egy rendszámtábla adatinak birtokába jutva hozzáférhettek egy webes API-hoz, amely kritikus funkciókat ért el, beleértve az ajtónyitást, motorindítást vagy nyomkövetést tett lehetővé. A sebezhetőséget egy kiberbiztonsági kutatócsapat fedezte fel, akik alapos vizsgálatok után kiderítették, hogy a Kia Connect szolgáltatás webes felülete nem megfelelően védett. A problémát a felhasználói adatkezelési hiányosságok okozták, amelyek lehetőséget adtak arra, hogy egy támadó pusztán a rendszámadatok beírásával lekérdezze a jármű azonosítóit és parancsokat adjon ki. A kutatók ezt követően azonnal értesítették a Kia-t, a gyártó pedig gyorsan befoltozta a biztonsági rést, minimalizálva a kockázatokat. Az eset azonban rávilágít arra, hogy az autóiparban a digitális rendszerek, különösen a webes API-k, vonzó célpontjai lehetnek a kibertámadásoknak. Ez a felfedezés része egy szélesebb körű vizsgálatnak, amely más autógyártók hasonló sérülékenységeit is feltárta, rámutatva az autóipar kiberbiztonsági kihívásaira és a biztonsági megoldások fejlesztésének fontosságára. [20]

1.2 Célkitűzés(ek)

Az információbiztonság növekvő szerepe a modern személygépjárművek működésében arra ösztönzött, hogy feltárjam azokat a tényezőket és szabályozási hiányosságokat, amelyek akadályozzák a járművek egységes informatikai eszközként való kezelését. A kutatás célja annak vizsgálata, hogy a jelenlegi jogszabályi környezet milyen mértékben és milyen területeken biztosít megfelelő védelmet a személygépjárművek számára mint integrált informatikai rendszerek. Ezen felül a kutatás azt is vizsgálja, hogy a felhasználók mennyire vannak tisztában járműveik adatkezelési és adattovábbítási gyakorlataival, valamint milyen biztonsági kockázatokat érzékelnek az adatkezelés átláthatóságának hiányában.

A kutatás specifikus célkitűzései az alábbiak szerint fogalmazhatók meg:

- A személygépjárművek informatikai eszközként való kezelésével kapcsolatos jogszabályi környezet elemzése, különös tekintettel az adatbiztonsági szempontokra.
- A személygépjárművek informatikai rendszereinek néhány biztonsági szempontból nem kielégítő megoldásának (weakness) feltárása, különös tekintettel az adattovábbítás során fennálló biztonsági kockázatokra.

- Annak vizsgálata, hogy a felhasználók mennyire vannak tisztában a járművük által végzett adatkezelési tevékenységekkel, és milyen tájékoztatási igényeik vannak.
- Egy átfogó kockázatmenedzsment keretrendszer szükségességének és lehetséges elemeinek meghatározása, amely figyelembe veszi a járművek adatkezelési, adattárolási és adattovábbítási folyamatait.

A kutatási célkitűzések eléréséhez az alábbi kutatási kérdések kerültek megfogalmazásra:

Azonosító	Kérdés
K1	Hogyan kezeli a jelenlegi információbiztonsági jogszabályi környezet a személygépjárműveket mint informatikai eszközöket?
K2	Milyen hiányosságok tapasztalhatók az információbiztonsági szabályozásokban a személygépjárművek átfogó kezelésére vonatkozóan?
K3	Hogyan használhatók ki a személygépjárművek informatikai rendszerei a felhasználó és a gyártó tudta nélküli adatküldésre?
K4	Milyen mértékben vannak tájékoztatva a személygépjármű-tulajdonosok a járműveik által végzett adattovábbításról?
K5	Hogyan érzékelik a személygépjármű-tulajdonosok a személyes adataik kezelésével kapcsolatos kockázatokat, és milyen tájékoztatási igényeik vannak?
K6	Milyen szerepet tölthet be egy felügyeleti hatóság a személygépjárművek adatbiztonságának biztosításában?
K7	Milyen elemekből állhat egy hatékony kockázatmenedzsment keretrendszer a személygépjárművek adatbiztonsága szempontjából?
K8	Hogyan javíthatja a kockázatmenedzsment keretrendszer a személygépjárművek adatkezelését és adattárolását?

2. táblázat - Kutatási kérdések megfogalmazása

A kutatási kérdések és célkitűzések együttesen arra irányulnak, hogy átfogó képet nyújtsanak a személygépjárművek információbiztonsági kihívásairól és szabályozási hiányosságairól, valamint olyan gyakorlati megoldásokat vizsgáljanak, amelyek a jövőben elősegíthetik a személygépjárművek biztonságosabb működését és a felhasználói tájékozottság növelését.

1.3 A téma kutatásának hipotézisei

A kutatási hipotéziseimet az alábbi táblázat foglalja össze:

Azonosító	Hipotézis
H1	Az információbiztonsági jogszabályok által támasztott követelmények nem fedik le a személygépjárművet egységes informatikai eszközként, hanem főként a gyártókat vagy egyes alrendszereket érintő problémákra fókuszálnak.
H2	A személygépjárművek, mint egységes informatikai eszközök, sérülékenyek lehetnek a hackertámadásokkal szemben, és általuk lehetővé válhat titkos adatküldés akár a felhasználó és a gyártó tudta nélkül.
H3	A személygépjármű tulajdonosok nem kapnak elegendő tájékoztatást a járművük által végzett adattovábbításról, így nincsenek tisztában a személyes adataik kezelésével kapcsolatos kockázatokkal.
H4	A személygépjárművek biztonságos informatikai eszközként való kezeléséhez átlátható adattovábbítási rendszer, titkosított adatforgalom és egy felügyeleti hatóság kijelölése szükséges.
H5	Egy átfogó kockázatmenedzsment keretrendszer, amely figyelembe veszi az adatkezelés, adattárolás és adattovábbítás valamennyi aspektusát, hatékonyan hozzájárulhat a személygépjárművek biztonságának növeléséhez.

3. táblázat - Hipotézisek összefoglalása

1.4 Kutatási módszerek

Mielőtt a kutatási módszereket részletesen tárgyalnánk, szót kell ejtenünk az értekezésben megjelenő főbb fogalmakról. Az "okosautó" és a korábbiakban használt "connected car" vagy összekapcsolt autó fogalom gyakran együtt jellennek meg a szakirodalomban, de az "okosautó" fogalma szélesebb körű jelentéstartalommal bír, magában foglalja az önvezető technológiát, mesterséges intelligenciát és az IoT (Internet of Things) egyéb elemeit is. Ezzel szemben a "connected car" specifikusan az internetkapcsolatot és az adatforgalmat érintő jellemvonásokat tömöríti.

A továbbiak során az alábbiak szerint érdemes értelmezni a definíciókat:

Az "okosautó" (smart car) és az "internetkapcsolatra képes autó" (connected car) fogalmai gyakran átfedik egymást és a szakirodalomban is sok esetben szinonimaként szerepelnek, de ezzel egyidőben fontos különbségek is vannak közöttük.

Okosautó (Smart Car)	**Internetkapcsolatra képes autó (Connected Car)**
Az okosautó olyan jármű, amely integrálja az IoT-eszközöket és intelligens rendszereket, lehetővé téve a jármű önálló érzékelését, kommunikációját és bizonyos szintű automatizációját. Ezek a rendszerek folyamatos adatforgalmat igényelnek, beleértve a helyadatokat, a jármű állapotára vonatkozó adatokat és az utasok adatait is. Az okosautók képesek valós idejű adatgyűjtésre és feldolgozásra, ami növeli a vezetés biztonságát és hatékonyságát. [21]	Az internetkapcsolatra képes autók olyan járművek, amelyek képesek adatokat küldeni és fogadni interneten keresztül, akár a gyártóval, akár más eszközökkel vagy szolgáltatásokkal. Ezek a járművek olyan funkciókat kínálhatnak, mint a valós idejű navigáció, távoli diagnosztika és a biztonsági funkciók felügyelete. A connected car technológia lehetővé teszi a járművek számára, hogy kommunikáljanak más járművekkel és az infrastruktúrával, növelve ezzel a közlekedés biztonságát és hatékonyságát. [22]

4. táblázat - Az okosautó és az internetkapcsolatra képes autó definíciós különbségei

Szintén fontos fogalmak az adatbiztonság és az adatvédelem. Az adatbiztonság és az adatvédelem szorosan összefügg, mégis fontos különbséget tenni a két fogalom között, különösen információbiztonsági kontextusban.

Adatvédelem	**Adatbiztonság**
Az **adatvédelem** főként a személyes adatok kezelésére, tárolására és megosztására vonatkozó szabályokat és elveket foglalja magában, célja pedig az, hogy megvédje az egyének magánéletét és személyes információit a jogellenes felhasználástól. Az adatvédelem alapját	Ezzel szemben az **adatbiztonság** az információk (beleértve a személyes adatokat is) védelmét célzó technikai és szervezeti intézkedések összessége. Az adatbiztonság fókuszában az adatok integritásának, hozzáférhetőségének és bizalmasságának fenntartása áll,

jogszabályok, például az Európai Unió általános adatvédelmi rendelete (GDPR) képezi, amelyek meghatározzák, hogy a szervezetek milyen módon gyűjthetnek, dolgozhatnak fel és tárolhatnak személyes adatokat, biztosítva az érintettek jogait és védelmét.	függetlenül attól, hogy azok személyes adatokat tartalmaznak-e vagy sem. Az adatbiztonság főként információbiztonsági szabványokra, például az ISO/IEC 27001-re épül, amely keretet biztosít a szervezetek számára a megfelelő védelmi intézkedések kialakításához, beleértve a hozzáférés-kezelést, titkosítást, biztonsági mentést és incidenskezelést. Míg az adatvédelem tehát jogi és szabályozási keretekkel foglalkozik, az adatbiztonság technikai megoldásokat és folyamatokat alkalmaz annak biztosítására, hogy az adatok mindenkor védettek maradjanak a jogosulatlan hozzáféréstől és a veszélyforrásoktól.

5. táblázat - Az adatvédelem és adatbiztonság fogalmi megkülönböztetése

Dolgozatom megközelítése alapvetően adatbiztonsági szempontból vizsgálja az internetkapcsolatra képes személygépjárműveket, illetve a jelenleg is elterjedt okos személygépjárműveket.

A dolgozat megírásához végzett kutatás a következő elemekből épült fel:

1. Kutatásom során megvizsgáltam a jelenlegi információbiztonsági környezetet a személygépjárművekre és a gyártókra vonatkozóan és megállapítottam hogy a jelenlegi szabályozások nem elégségesek az úgynevezett okosautók adatcseréjének megfelelő kontrollálásához.
    a. A jelenlegi szabályozás nem kezeli a személygépjárművet egységes informatikai eszközként, amely alapfeltétele lenne a megfelelő kontrollnak.
    b. A jelenlegi szabályozás nem ír elő kötelező feltételeket az adatok küldésének szabványos módjával kapcsolatban.

c. A jelenlegi szabályozás nem teszi kötelezővé az adatcsere módjainak publikussá tételét.

2. Kérdőíves kutatást készítettem, melyben 289 személyt kérdeztem meg az okosautókkal kapcsolatos tapasztalatairól. A kérdőívet magyar és egyéb országokból származó személyek is kitöltötték.
    a. Megállapítást nyert, hogy a felhasználók nem kapnak tájékoztatást az adataik kezelésével kapcsolatban, vagy nem megfelelő módon kapják meg azt (nem tudnak róla, elsiklanak felette).
    b. A felhasználók fontosnak tartják az adatáramlás átláthatóságát és igénylik a tájékoztatást erre vonatkozóan.
3. Mélyinterjút készítettem 10 magyarországi kiemelt szakértővel amellyel a személygépjárművek adatküldésének információbiztonsági szintjét vizsgáltam.
    a. Megállapítottam hogy nincs elfogadott és egységes gyakorlat a követendő irányelvekkel kapcsolatban.
4. Megvizsgáltam a rejtett adatküldés mennyiségének gyakorlati vonatkozásait, feltételezve, hogy a személygépjármű vagy annak valamely egysége kompromittált. Arra jutottam, hogy számos szolgáltatás képes lehet megfelelő mennyiségű rejtett adatot továbbítani.
    a. Megállapítottam, hogy az okos járművek alapvető szenzorai képesek lehetnek havonta egy-két fénykép (utcakép) illetve néhány perces hangfelvételek elküldésére. Az állításomat számításokkal igazoltam.
    b. Megállapítottam, hogy az okos járművek kényelmi funkciói (p. önvezető modul) jelentős mennyiségű rejtett adat küldésére lehet alkalmas (pl. napi több utcakép). Az állításomat számításokkal igazoltam.

Az okosautók elterjedését és gyors evolúcióját, illetve az új, korábban ismeretlen szereplők felbukkanását figyelembe véve az európai piacon következtetéseket vontam le a jövő személygépjárművének kihívásait illetően. Megállapítottam, hogy az okosgépjárművek egyre jobban fokozott kiemelt célpontjai lesznek a kiberbűnözőknek, kormányzati hacker csoportoknak.

2. A TÉMA RELEVANCIÁJA: GEOPOLITIKAI ÉS GAZDASÁGI KONTEXTUS

Az Európai Unió az elmúlt években sokat tett mind az adatvédelem, mind pedig a kiberbiztonság fokozásáért. Ennek legutóbbi eredménye a NIS2 kiberbiztonsági keretrendszer bevezetése, amit minden tagállamnak kötelező átültetnie a saját jogrendszerébe és amely részletes követelményeket ír elő a piaci és állami szervezetek egy jelentős részének. Ezenkívül számos más olyan törekvés létezik, amely szintén ezt a célt hivatott támogatni, mint például a TISAX megjelenése és terjedése, azonban ezek – bár elvi szinten hasonló tartalommal rendelkeznek és hasonló alapokon nyugszanak, – nem alkotnak egy egységes védelmi rendszert és a betartatásuk is kihívást jelent. Ez főleg abban a tekintetben igaz, amikor nem egy adott szervezetet vagy egy adott szolgáltatást, illetve informatikai terméket veszünk alapul, hanem egy olyan komplex, számtalan beszállító alkatrésze, munkája által előállított terméket, mint amilyen a személygépjármű.

A NIS2 irányelv bevezetése a dolgozat írásakor is folyamatban van az egyes tagállamokban, azonban az a trend már látható, hogy a helyi jogszabályi környezetbe való implementálása minden országban nagyon eltérő, főként a már kialakult gyakorlatokon alapszik. Hazánkban például a NIST SP 800-53 Rev. 5. amerikai ajánlás alapján valósul meg, míg Németország az ISO27001-hez hasonló megközelítést alkalmaz. Fontos megjegyezni azt is, hogy a NIS2 irányelv nem vonatkozik (vagy csak közvetetten érinti) az Európán kívüli gyártókra, betartatása pedig a bonyolult nemzetközi összefontódások esetében (harmadik országbeli anyavállalat, ázsiai ellátási lánc szereplők) nehézségekbe ütközik.

2.1 Az Európai Unió helyzete a járműipari információbiztonság terén

Az Európai Unió felkészültsége információbiztonsági szempontból jelenleg nem megfelelő ahhoz, hogy hatékonyan védje az állampolgárok adatait vagy a személygépjárművek esetében akár testi épségét az esetleges hibákkal vagy visszaélésekkel szemben. Az elmúlt években – főként a GDPR megjelenésének hatására – jelentek meg azok a fejezetek a szabványokban, amelyek már kifejezetten az adatvédelemmel foglalkoznak, és gyakorlati útmutatásokat tartalmaznak arra vonatkozóan, hogy miként kell eljárnia a szabványt alkalmazóknak az ügyfeleikkel vagy más érintettekkel kapcsolatban. Jó példa erre a NIST SP 800-53 Rev. 4. (eredeti

megjelenés: 2014) és a NIST SP 800-53 Rev. 5. (eredeti megjelenés: 2020) közötti különbség, amely egyebek között abban nyilvánul meg, hogy a 2020-as szabványban külön új kontrollcsaládként jelenik meg az adatvédelem.

A személygépjárművek védelme azért kiemelten fontos, mert napjainkban a mobiltelefonokhoz hasonlóan képesek a felhasználó szinte minden adatának gyűjtésére, illetve egyre nagyobb százalékban rendelkeznek olyan fedélzeti rendszerekkel, amelyek internetkapcsolatra is képesek. Ez különösen igaz az elektromos járművekre, hiszen itt a fogyasztás optimalizálásának sokkal jelentősebb szerep jut. Ennek megfelelően a mobiltelefonokhoz hasonlóan (és a tradicionális személygépjárművekkel ellentétben) könnyebben feltörhetővé válnak anélkül is, hogy a támadónak fizikailag meg kellene közelítenie őket. Az ilyen támadásokra jó példa lehet Sam Curry webalkalmazások biztonságával foglalkozó kutató 2023. január 3-ai esettanulmánya [23], amelyben részletes leírást ad több ismert márka rendszereihez való távoli hozzáférés lehetőségeiről. A teszt során Curry és csapata a következő adatokhoz fért hozzá a teljesség igénye nélkül: a tulajdonos elérhetőségei, e-mail-címe, telefonszáma (pusztán az alvázszám ismeretében), és a következő rendszereket volt képes távolról irányítani: elektromos zár, motor (indítás is), precíziós lokáció, fényszórók, duda, a felhasználói fiók lecserélése (azaz a felhasználó kizárása az autóból), hozzáférés a 360 fokos kamerához élő felvételek készítésével, távoli kódok futtatása, hozzáférés a memóriák tartalmához, illetve egyes márkák esetében hozzáférés a vállalat dolgozóinak adataihoz.

Ahogyan más iparágakban, a személygépjárműgyártó iparnak is vannak olyan specifikus információbiztonsági szabványai, amelyek kifejezetten a kibervédelemre fókuszálnak, azonban ezek vizsgálati tárgya szinte soha nem maga az összetett végtermék egyben, még csak nem is a felhasználó adatvagyona, hanem a gyártó vagy a beszállítók folyamatmenedzsmentje, a működés során alkalmazott alapelvek. Bár napjainkban már az általános információbiztonsági szabványokban is egyre nagyobb hangsúlyt kap az adatvédelem, az elvek fő forrása még mindig a GDPR, így az erre vonatkozó kontrollok nem mondják ki, hogy hogyan kell megvalósítani a biztonságot, hanem csak az elvárásokat fogalmazzák meg.

Az elmúlt években azonban ezen a területen javulás tapasztalható, hiszen elkezdtek megjelenni a kifejezetten kibervédelmi szemléletű biztonsági szabványok, amelyeket specifikusan az autóiparra alkalmazhatnak a szakemberek. Ilyenek például a TISAX (2017) vagy az ISO/SAE 21434 (2021). A 2. táblázatban felsorolunk néhány szélesebb

körben is alkalmazott szabványt, amelyek követelményei kiterjednek a személygépjárműgyártókra és az ellátási láncra is. Bár ezek a szabványok egyre inkább elterjedtek, és például az ISO 27001-nek a piaci elfogadottsága is magas, nem kötelező érvényűek, és a gyakorlatban nem mindig alkalmazzák őket kellő mélységgel. Problémát okoz az is, hogy ezeknek a szabványoknak a nagy része a folyamatokra vagy a gyártóra koncentrál, illetve hogy a biztonsági értékelés komplexitása ellenére nagyrészt *ad hoc* jellegű. Minél összetettebb rendszerről van szó, annál nehezebb pontos metrikát alkalmazni a kockázatok elemzésére [24], [25]. A szakértők szubjektív ítéletei fontos információkat szolgáltatnak a kiberfizikai rendszerek fenyegetéseinek értékelése és modellezése során, azonban a legtöbb szakértőben valamilyen mértékű bizonytalanság rejlik az értékelések terén [26].

2.2 Kína, mint az Európai Unión kívüli piaci szereplő megjelenése

A Kínai Népköztársaság elektromos személygépjármű-iparában elért sikerek stratégiái és programjai

2010-ben az Államtanács kiadta *A stratégiai feltörekvő iparágak kifejlesztésének és fejlesztésének felgyorsításáról* című döntést, amelyben az elektromosjármű-ipart, az energiahatékonysági ipart, a környezetvédelmi ipart és más kapcsolódó iparágakat a stratégiai feltörekvő iparágak közé sorolta Kínában [27]. A stratégiai feltörekvő iparágakat olyan iparágaknak tekintik, amelyek hatalmas technológiai innovációs potenciállal rendelkeznek, és fejlődésük korai szakaszában vannak. Nyilvánvaló, hogy a nemzeti szintű politikai ösztönzők és hatások tanulmányozása fontos elméleti és gyakorlati jelentőséggel bír. Az elektromos járműipar egy tipikus példája a stratégiai feltörekvő iparágaknak Kínában, amely kiemelt szerepet kapott Kína gazdasági és technológiai fejlődésének irányításában az elmúlt évtizedben [28]. Az iparág azóta – köszönhetően a kapcsolódó programoknak és politikáknak – sokat fejlődött, jelenleg a technikai és kereskedelmi bemutató szakaszban tart.

Kína Államtanácsa az elmúlt évtizedben számos irányelvet jelentetett meg az elektromos járművek (EV-k) gyártásának és értékesítésének felgyorsítására, valamint a kapcsolódó töltő-infrastruktúra kiépítésére vonatkozóan is. A Nemzeti Fejlesztési és Reform Bizottság (National Development and Reform Commission – NDRC), a Pénzügyminisztérium, az Ipari és Informatikai Minisztérium (Ministry of Industry and Information Technology – MIIT), a Tudomány és Technológia Minisztériuma (Ministry

of Science and Technology – MST) és más illetékes hatóságok együttesen cselekedtek, hogy különféle politikákat vezessenek be, például *pilot*programokat szervezve, kutatás-fejlesztésbe fektetve, EV-vásárlási támogatásokat bevezetve, adókedvezményeket és mentességeket nyújtva, könnyű piaci hozzáférést és infrastruktúra-építést biztosítva [29]. Az alábbiakban ezek közül emelünk ki három fontos tartópillért: a fenntarthatóságot, a kutatás-fejlesztést és a piacot célzó programokat és politikákat. Fontos megjegyezni, hogy a tanulmány nem törekszik a programok és politikák teljes körű bemutatására, hiszen az meghaladná annak kereteit, hanem csak egy vezérfonalat kíván felmutatni a legnagyobb hatású intézkedések alapján.

2.2.1 Fenntartható közlekedési rendszer kialakítása

Az elektromos járművek népszerűségének növekedése a klímaváltozásra adott válaszokkal szorosan összefonódva jelenik meg a politikai térben. A Kínai Népköztársaság ennek megfelelően stratégiai döntéseket hozott a fenntartható közlekedési rendszer kialakítására, ami jelentős hatással bírt az elektromos személygépjárművek fejlesztésére. Az ország hosszú távú tervei közé tartozik a fosszilis üzemanyagok függőségének csökkentése és az alternatív hajtású járművek terjedésének előmozdítása. Ennek érdekében a kínai kormányzat különböző programokat és ösztönzőket vezetett be az elektromos járművek gyártására és vásárlására.

Kína továbbra is az első helyet foglalja el a globális energiaigény növekedésében és az energetikához kapcsolódó kibocsátásban, amely a globális nettó energiaigény-növekedés 90%-át teszi ki [30]. Ez szorosan összefügg azzal a ténnyel, hogy Kína energiaszerkezete részben a szénre és alacsony kihasználtsági hatékonyságra épül. A közlekedési iparág vált a világ fő energiafogyasztási és szennyezőanyag-kibocsátási forrásává. Kína közlekedési iparában az energiafogyasztás évente közel 10%-kal nőtt, a teljes energiafogyasztás közel 15%-át teszi ki. 2019-ben az országos járműállomány száma elérte a 348 milliót, ami 6,4%-os növekedést jelentett az előző évhez képest. Közülük az „új energiás járművek” (NEV-ek – azaz *new energy vehicles*) száma elérte a 3,81 milliót. Az országos járművek négy értékelt szennyező anyagának teljes kibocsátása 16 038 kt volt; a benzines járművek CO2-kibocsátása meghaladta a teljes járműkibocsátás 80%-át; a szénhidrogén-kibocsátás pedig 70%-kal haladta meg a szennyezési határértéket a Kínai Közlekedési Forrás Környezetvédelmi Menedzsmentjének éves jelentése alapján [30].

Az utóbbi években Kína kormánya ennek megfelelően szorosan koordinálta a megújuló energiák és az autók elektromosításának felhasználását az energiaágazatban. A cél az

energiafogyasztás és a szennyezőanyag-kibocsátás csökkentése a közlekedési iparban. Általában véve, a járművek számának folyamatos növekedésével Kína összesített energiafogyasztása és kibocsátása emelkedő tendenciát mutat. Mint a mindennapi életben fontos közlekedési eszközt, 2019-ben 21,36 millió személyautót gyártottak és értékesítettek az országban, amivel továbbra is az első helyen áll a világon. Ezért rendkívül fontos az energiahatékonyság és a piaci struktúra javítása, valamint a kibocsátási tényező csökkentése. [30]

A kínai kormány ezekre a problémákra válaszul két környezetbarát NEV-bemutatóprojektet indított a járművek kereskedelmi hasznosításának elősegítése érdekében. Az első kör 2009 januárjától 2012 decemberéig tartott, és többek között Pekinget, Sanghajt, Hangzhout, Daliánt és Sencsent, összesen 25 *pilot*várost foglalt magába. A bemutató projekt kezdetben a közösségi területekre (buszok, speciális járművek) összpontosított, majd 2010 májusától kiterjesztették a magánjellegű területekre is. Az első kör bemutató projektének eredményei messze elmaradtak az elvárásoktól, ezért a kínai kormány kiadta a *Folytatott munka az új energiás járművek fejlesztésének elősegítése érdekében* című közleményt, amelyben döntöttek a bemutató projekt következő három éven át történő folytatásáról, ami a második kör NEV-bemutatóprojektjeként vált ismertté. A második körös projekt 39 városcsoportot, összesen 88 várost foglalt magában [32].

2020. november 2-án a Kínai Népköztársaság Államtanácsának Hivatala közzétette az Új NEV Fejlesztési Tervét (2021–2035). Ez a tervezet a legfelsőbb szintű stratégiai irányelveket foglalja magában, amelyek a következő 15 év során Kínában egy átfogó és teljesen integrált Új NEV és Intelligens Kapcsolódó Jármű (ICV – *intelligent connected vehicle*) ökoszisztéma fejlesztését irányítják. A terv ugyanakkor része annak az átfogó útnak, amely során Kínát globális autóipari nagyhatalommá kívánják fejleszteni. A terv a 2012–2020 közötti Energiamegtakarítási és Új Energiajármű-ipar Fejlesztési Tervet követi, amelyet 2012-ben adott ki az Államtanács [33].

2.2.2 Kutatás-fejlesztés és technológiai innováció

A kínai elektromos személygépjármű-ipar sikereiben kulcsszerepet játszott a kutatás-fejlesztés és a technológiai innováció. A kormányzati támogatás és az iparági partnerségek révén a kínai autógyártók jelentős előrelépést tettek az akkumulátortechnológia fejlesztésével kapcsolatban, a hatékonyság növelésében és az elektromos járművek egy töltéssel bejárható tartományának megnövelésében. Emellett a

Kínai Népköztársaság kiemelt figyelmet fordított a töltő-infrastruktúra fejlesztésére is, amely elengedhetetlen a töltési kényelem és a felhasználói elfogadás szempontjából. Terjedelmi okokból kifolyólag jelen tanulmányban a töltő-infrastruktúrával kapcsolatos témaköröket nem fejtjük ki bővebben, azonban lényeges megjegyezni, hogy azok szerves részét képezik az elektromos járművekkel kapcsolatos minden stratégiának, programnak és gazdasági intézkedésnek. Az infrastruktúra szerepe, hogy csak néhány területet említsünk, fontos az értékesítés, az energetika és a nemzetbiztonság szempontjából is.

Az elektromos személygépjármű-ipari politika legfontosabb funkciója az erőforrások irányítása. Az új energiával működő autóipar politikája fokozatosan átalakul „kormányvezérelt" megközelítésből a „piacvezérelt" megközelítés felé. Ennek megfelelő arányairól és a várható hatásokról számos szakmai publikáció született.

Xu és munkatársai tanulmánya [34] egy olyan új típusrendszert javasol ennek megközelítéséhez, amely a kormány választása versus a piac választása és a termelőorientáció versus fogyasztóorientáció dimenziókra osztja az innovációs politikai eszközöket. A kínai kormányzati politikák az új energiával működő járművek iparában is fokozatosan változnak a „kormány választása" felől a „piac választása" felé. Ji és munkatársai [35] a töltőoszlopok telepítési politikáját tanulmányozták Kínában, és úgy vélték, hogy az elektromos autók nagyarányú használata az infrastruktúra kiépítésével kapcsolatos szoros összefüggések miatt csak a kormány irányítása alatt lesz kivitelezhető. Andersen és munkatársai [36] egy intelligens újratölthető hálózatot, vagyis „elektromos újratöltőhálózat-üzemeltető" (*electric recharge grid operator* – ERGO) modellt javasoltak. Az ERGO üzleti modell egyszerre lenne képes megoldani az új energiával működő járművek használatából eredő ellátási ingadozásokat és a közlekedési kibocsátási problémát.

A szakirodalomban gyakran visszatérő elem, hogy úgy tűnik, hogy a kínai gyártók képesek innovációkat előállítani még nagy társadalmi és gazdasági átalakulás közepette is. Azonban sokan azt állítják, hogy az innováció hajtóereje nem ennek ellenére, hanem éppen ezekben a körülményekben rejlik. Néhányan, például David Chao, a Doll Capital Management képviselője, azt állítják, hogy az innovációs kapacitás forrása a kínai piac rendkívül árérzékeny jellege [37]. Mások az innováció sajátosságaira mutatnak rá, és azt állítják, hogy a sikeres stratégiai innovációk általában kis, alacsony nyereségű vállalkozásokból indulnak, majd növekednek, amíg el nem érik a forradalmi pontot, amit a már régóta a piacon lévő, rugalmatlanná vált nagy szereplők nehezen tudnak követni

[38] Így nem meglepő, hogy az új gazdaságok közül Kína az ilyen innovációk legfőbb forrása [39].

Hogy honnan ered a kínai vállalatok erős innovációra való hajlama, és milyen eredményei vannak ennek, arról sokféle különböző véleményt olvashatunk a szakirodalomban. Néhány szakértő az innováció kínai sajátosságait tanulmányozta – mint például Li és munkatársainak tanulmánya [40]; Krug [41]; Krug & Hendrischke [42]; Krug & Polos [43] – azt sugallják, hogy az innováció valójában egy rendszerszintű válasz a bizonytalanság magas fokára és a vállalkozók érdekei ellen ható helyzeti korlátokra. Ezzel némileg ellentétben Jin és Li [44] tanulmányozta a vállalatok tulajdonjogi struktúrája (állami vagy magánszféra) és az új termékfejlesztés közötti kapcsolatot, és arra a következtetésre jutottak, hogy a kínai piaci környezet inkább lehetővé tevő, mintsem gátló az új termékfejlesztési projektek szempontjából. Wang és Kimble [45] a BYD példáján mutatták be ezt a folyamatot cikkükben. Kutatásaik alapján egy általános jelenségre hívják fel a figyelmet: a General Motors és a Toyota sem tudta fenntartani a BYD-nél tapasztalható magas vertikális integrációs szintet egy bizonyos szint elérése után. Az elektromos járművek gyártójaként a BYD jövőbeli életképességének legkritikusabb kérdése a kutatók szerint ebből kiindulva az, hogy képes-e önerőből, a piacra támaszkodva folytatni az innovációk sorozatát, amelyek lehetővé tették, hogy a konkurenciát megelőzze mind az akkumulátorok, mind pedig a hagyományos autók területén. A BYD eddigi sikere a Beaume és Midler [46] által „radikális fokozatosságnak" nevezett módon épült, de az évek során a cég földrajzilag és termékpalettában is diverzifikálttá és jelentős vállalkozássá vált. A Chery, a Geely és más vezető kínai autógyártók hasonló dinamikát mutatnak [47]. Az általánosan megfigyelhető jellemzőkön kívül fontos még szót ejteni a kvázi nyílt moduláris termékarchitektúrák elterjedéséről is, amelyek alkalmazása más vezető vállalatok esetében is gyakori. A termékarchitektúra ezen különlegesnek mondható formájának nagyvállalati alkalmazása csak Kínában figyelhető meg [47].

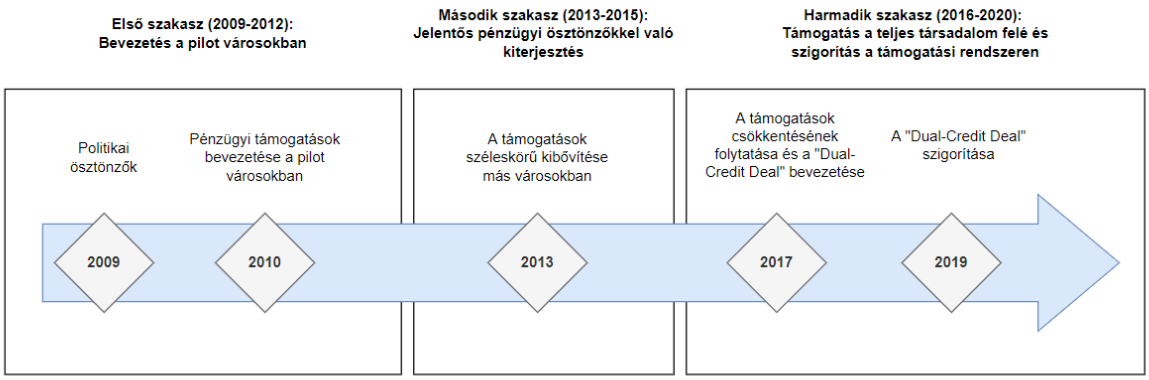
2.2.3 Piaci szabályozás és támogatások

A kínai kormányzat számos piaci szabályozással és támogatási programmal ösztönözte az elektromos járművek gyártását és terjedését. A járműgyártóknak például kötelező kvótákat kellett teljesíteniük az elektromos járművek értékesítésére, amelyek elősegítették az ipar fellendülését. Emellett adókedvezményeket, vásárlási támogatásokat

és a töltési infrastruktúra kiépítéséhez nyújtott állami támogatásokat is biztosított számukra.

Kínában az elektromos járművek országos iparosodása és kereskedelmesítése 2009 elején kezdődött. A pénzügyi támogatások nyújtása révén először a tömegközlekedés, majd a magánfogyasztás területén, és az urbanizációs kísérletektől a régiós kísérleteken át a nemzeti szintű promócióig fokozatosan haladt előre. Ennek a szerteágazó, lépcsőzetesen építkező politikának az volt a célja, hogy ösztönözze a beruházásokat, elősegítse az ipari növekedést, és csökkentse az indulási időszak nehézségeit. Ezzel egyidőben a támogatásokat fokozatosan, fázisokban tervezték megszüntetni és a hozzáférhetőségüket jellemző jogosultsági küszöböt fokozatosan emelni. Ehhez olyan ipari klaszterek létrehozására volt szükség, amelyek globális versenyelőnnyel rendelkeznek. A támogatási politikáknak három különböző módosítási szakaszon kellett átmenniük az ipari fejlődés érdekében.

A 2012-ben kiadott *Az elektromos járművek fejlesztésének 12. ötéves tervé*ben (China: 12th Five-Year Plan) Kína hivatalosan javasolta az elektromos járművek iparosítása lépcsőzetes stratégiájának végrehajtását, és három fázisra osztotta a folyamatot. Az I. fázis 2009–2012 között zajlott le; a II. fázis 2013–2015 között; a III. fázis pedig 2016–2020 között[48].



1. ábra A kínai nemzeti ösztönzők bevezetésének mérföldkövei az elektromosjármű-iparban

A *Dual-Credit Deal* rendszer 2017/2018-as bevezetése egy új kísérletet jelentett a Kínában működő NEV-járműpiac fejlesztése számára. A rendszer bevezetése óta az új energiával működő autóipar egyrészről gyorsan fejlődött, másrészről pedig sok autógyártó cég nehézségekkel küzdött. Yang és munkatársai [49] a 2012 és 2019 közötti

időszakban a kínai személyautóval foglalkozó vállalatok adatai alapján a *Dual-Credit* rendszer hatását vizsgálták vállalati szinten. Az elemzés során először azt találták, hogy a NEV-vel foglalkozó vállalatok teljesítménye csökkent a rendszer bevezetése miatt. Ráadásul a kutatás-fejlesztési beruházások súlyosbíthatják a *Dual-Credit* rendszer negatív hatásait a vállalati teljesítményre nézve. Végül összehasonlítva a magánvállalatokkal a központi állami vállalatok érzékenyebben érintettek a *Dual-Credit* rendszer által.

A kormányzati beszerzés és a pénzügyi támogatás fontos szerepet játszottak az EV-k kereskedelmi forgalomba hozatalának előmozdításában és a gyártók lelkesedésének felkeltésében [50]. Különösen azóta, hogy 2016 óta fokozatosan pénzügyi támogatásokat vezettek be, nagy növekedés tapasztalható az EV-k gyártása és értékesítése terén. Ez is bizonyította az EV-gyártók pénzügyi támogatásokra való támaszkodását [51].

2.2.4 Az ösztönzők sikere és a felmerülő kihívások

A jelen fejezetben bemutatott ösztönzők elemzése alapján tehát ellentmondásos kép rajzolódik ki azok hatásosságát illetően. A kutatók összességében egyetértenek abban, hogy a sikeres programok ellenére is jelentős és világviszonylatban unikális kihívásokkal néz szembe a kínai elektromos személygépjármű-ipar és -piac. A vállalatok egyre inkább kénytelenek a keresletre támaszkodni, miután a jelentős támogatásoknak köszönhető gyors növekedési ütem miatt az adaptációra fordítható idejük lecsökkent. Ezeknek a kihívásoknak a kezelése kimagasló tervezést és fokozott piaci növekedést kíván.

Az elektromos járművek iparának kezdeti sikereiben tehát döntő szerepet játszott az állami támogatás és a politikai akarat. A kínai kormányzat elkötelezetten támogatta az elektromos járművek terjedését és a hozzájuk kapcsolódó iparágak fejlődését. Az állami támogatások és ösztönzők segítették az elektromos járművek vásárlói és gyártói költségeinek csökkentését, valamint elősegítették a töltési infrastruktúra kiépítését. Összességében a Kínai Népköztársaság elektromos személygépjármű-iparának sikerei a komplex stratégiai és gyakorlati programok halmazán alapulnak. A fenntartható közlekedési rendszer kialakítása, a kutatás-fejlesztés és a technológiai innováció, a piaci szabályozás és támogatások, a nemzetközi együttműködés és piacra lépés támogatása, valamint az állami ösztönzők és politikai akarat mind-mind hozzájárultak ahhoz, hogy Kína az elektromos járművek piacának globális vezetőjévé váljon.

Kínai kutatók rámutattak, hogy ezek az intézkedések azonban nem feltétlenül hozzák majd el a várt eredményeket. Wu és munkatársai matematikai modellt fejlesztettek ki a *Dual-Credit* politikai rendszer hatásának metrikai meghatározására [48]. Szimulációs eredményei jelentős különbséget mutatnak a legutóbbi EV-értékesítés és az új politikai rendszer alapján szükséges becsült jövőbeli EV-termelés között. Az ilyen jelentős különbség azt sugallja, hogy jelentős politikai nyomás és elkerülhetetlen végrehajtási kihívások merülnek fel az utóbbi időben szigorodó *Dual-Credit* rendszerrel kapcsolatban. Mock és Yang [52] azt próbálták felmérni, hogy hogyan reagálnak az adóösztönzőkre a PHEV-k *(plug-in hybrid electric vehicle)* a világ vezető járműpiacain, azonban csupán néhány adatot és tényt soroltak fel, és nem végeztek matematikai elemzést. Lieven [53] húsz országban, öt kontinensen végzett felmérései arra utalnak, hogy az autópályákon a töltőhálózat kiépítése szükséges ahhoz, hogy a piac növekedése fellendüljön. Azonban mindezek a felmérések csak az ösztönző politikákra összpontosítottak anélkül, hogy figyelembe vettek volna más társadalmi-gazdasági tényezőket. Ráadásul az „attitűd-cselekvés" szakadék miatt a felmérések eredményei nem feltétlenül egyeznek meg az elektromos járművek valóságos vásárlói igényeiből kikövetkeztethető adatokkal.

A kínai nemzeti ösztönzők bevezetésének I. fázisában városi területeken indítottak *pilot*projekteket, amint azt az 1. táblázatban összefoglaljuk. A legtöbb *pilot*városban hibrid elektromos járműveket használtak a demonstrációs projektekhez. Azonban a technológiai készségek és az erőforrások hiánya akadályt jelentett a projektek sikeres véghezvitelében [54] [55]. A pénzügyi támogatások főként a közlekedési szektorokra összpontosultak, és ezek az ösztönzők alacsonyabbak voltak, mint amire a piac számított. Egy 2020-ban megjelent tanulmány [56] áttekinti a kínai autóipar nagymértékű elektromosítási ambícióinak hatását a 2021–2023-as időszakra nézve. A kutatás a *New Energy and Oil Consumption Credits* (NEOCC) modellt használja, egy olyan gépjármű-politikai elemzési eszközt, amelyet az Oak Ridge National Laboratory fejlesztett ki, hogy rendszerszinten kvantitatívan mérje a *Dual-Credit* rendszer potenciális hatásait a 2021–2023-as időszakra vonatkozóan. Ez a tanulmány megállapította, hogy a politika hatása alatt a kis üzemanyag-fogyasztású hagyományos járművek értékesítése gyorsabban növekedik, mint a 2018–2020-as időszakban, és az elektromos járművek (PEV-k) részesedése elérheti a 11,4%-ot 2023-ra, ha az 2017-es bővülést fenntartják (jelenleg tudjuk, hogy ezt az optimista becslést is meghaladta a valós adat [57]). Emellett a hosszú hatótávolságú elektromos járművek (pl. 400 km-es hatótávolságú BEV-k) és a *plug-in*

hibrid SUV-k lennének a legnépszerűbb PEV-típusok. Bár ez a tanulmány csak a kínai belső piacra összpontosít, az eredmények a nemzetközi piacra lépés szempontjából is relevánsak. A kutatók többek között a következő megállapításokat teszik a NEOCC-modell szimulációs eredményei alapján:

1. A megújult *Dual-Credit* politika (2021–2023) több eladást eredményezhet a magas üzemanyag-hatékonyságú járművek piacán, összehasonlítva a korábbi NEV-szabályokra fókuszáló *Dual-Credit* politikával szemben.
2. A tanulmány előrevetítette, hogy a politika korlátjai között bizonyos elektromos személygépjárművek részesedése a személygépjármű-piacon akár 11,4%-ra emelkedhet 2023-ig. (A becslés beigazolódott, sőt az adatok meghaladták ezt).
3. A hosszabb elektromos hatótávval rendelkező gépjárművek (például a 400 km-es hatótávval rendelkezők) lesznek a legnépszerűbbek 2021–2023 között.

Az eredmények alátámasztásához jelenleg még nem áll rendelkezésre elegendő adat, de amennyiben a számítások beigazolódnak, akkor elmondható, hogy a nehézségek ellenére a kínai autóipar növekedése nem áll meg, hiszen a politika és a piac viszonylagos összhangban képes egyszerre támogatni ezt a folyamatot.

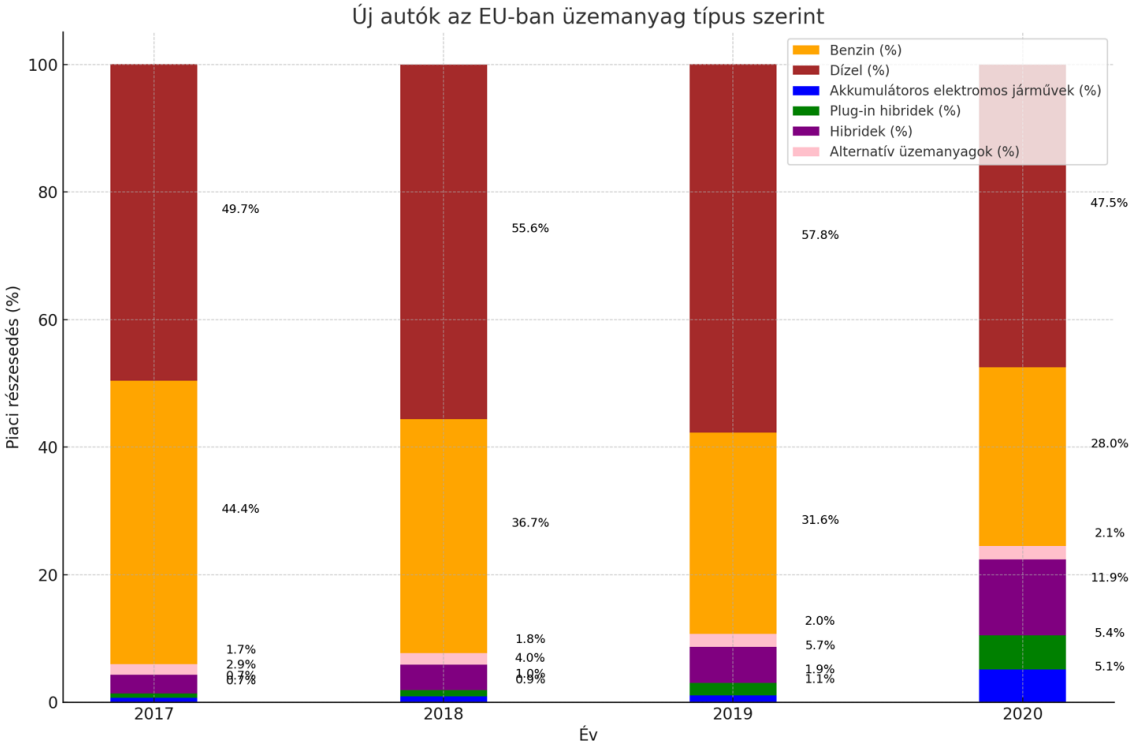
Fontos megjegyezni, hogy ezek a következtetések olyan feltételezéseken alapulnak, hogy az elektromosjármű-eladások a korábbi adatokhoz képest továbbra is folyamatosan növekednek. Figyelembe véve, hogy a járműpiac súlyos visszaesést tapasztalt 2018 és 2019 során, valamint a Covid-19-járvány által okozott bizonytalanságokat, még mindig nyitott kérdés a kutatók számára, hogy az elektromosítási átmenet folyamatosan bővül-e ezen a gyorsan fejlődő piacon.

2.2.5 Európai piacralépés

2021-től kezdve az Európai Unióban jelentősen megnőtt az elektromos járművek regisztrációinak száma [58]. 2021-ben az elektromos járművek (BEV-k és PHEV-k) részaránya az új személygépkocsik nemzeti nyilvántartásba vételében minden országban (EU-27, Izland, Norvégia) nőtt 2020-hoz képest. A legmagasabb arányt Norvégiában (86%), Izlandon (64%), Svédországban (46%) és Dániában (35%) mérték.

Németország, Franciaország és Norvégia a BEV-regisztrációk mintegy 63%-át adta (az EU-27 és az EU-n kívüli EGT-országok esetében). Norvégiában, abban az országban, ahol 2021-ben a legtöbb elektromos autót helyezték forgalomba, a BEV-k az új autóeladások 65%-át tették ki abban az évben. Néhány más európai országban azonban a

BEV-regisztrációk aránya a teljes flotta 1%-a körül maradt (Ciprus, Lengyelország, Csehország és Szlovákia). A PHEV-eladások aránya Izlandon (36%), Svédországban (25%) és Norvégiában (22%) volt a legmagasabb [58].



2. ábra - Új személygépjárművek üzemanyagtípus szerint 2017–2020 között

Az ACEA [59] információi alapján a hagyományos üzemanyagtípusú személygépjárművek száma fokozatosan visszaszorul, míg az új típusú üzemanyagokkal meghajtott járművek száma emelkedik. Európa jelenleg vonzó piac a kínai személygépjármű-gyártók számára, hiszen az elektromos járművek elterjedése gyors, azt az Európai Unió is specifikusan erre a célra kialakított programokkal támogatja, illetve fontos szempont, hogy a nyugati EV-k a kínaiak által kínált modelleknél jellemzően magasabb árakon érhetőek el. Az európai kormányzati támogatás és a kínai kormányzat export felé irányuló támogatása együttesen tovább ösztönzi ezeknek a márkáknak a belépését a régióba. Az új versenyzők az európai piac sajátosságainak megfelelően prioritást tulajdonítanak termékeik biztonságának és minőségének, amelyeket kifejezetten az európai fogyasztói preferenciákra terveznek. A kínai OEM-ek (*original equipment manufacturer*, azaz a márkák mögötti gyártók) alacsonyabb költségbázisa és a gazdaságosság révén általuk élvezett méretgazdaságosság előnyt jelent, amelyet a jövőben potenciálisan kiaknázhatnak. A magánhasználat mellett a flotta-/bérlési piac kulcsfontosságú célterület számukra [60].

Tíz járműcsoport felel a kínai személyautó-export 90%-áért, ezek közül azonban nem mindegyik aktív az európai piacon. A SAIC, az MG és a Maxus, valamint a Geely, amelyeknek márkaválasztékába tartozik a Polestar és a Lynk&Co, az elsők között jelentek meg az európai piacon. A Dongfeng európai jelenlétét az DFSK és a Voyah márkák segítségével építi ki. Jelentős résztvevőkként a Great Wall és a BYD jelenlegi terveikkel a gyors bővülésre törekszenek. A Changan, a Chery és a BAIC pedig még egyelőre kevés vagy semmilyen jelenléttel nem rendelkezik az európai országok piacain, de mindegyiknek vannak már olyan, specifikusan a helyi preferenciákhoz alakított márkái és termékei, amelyek lehetővé tehetik a későbbi belépést. A jelentős gyártókon kívül számos kisebb szereplő is megjelent már, például az Aiways, a Nio és a Xpeng, amelyek először az észak-európai piacokon próbálják megvetni a lábukat, és itt főleg a Teslával, valamint egyéb prémium német gyártókkal szemben veszik fel a versenyt [60]. Ezek alapján elmondható, hogy összességében a kínai márkák a piacralépés korai szakaszában vannak, így túl korai lenne, és túl sok tényezőt érintene, hogy reálisan értékeljük a lehetséges nyerteseket és veszteseket.

Az Európai Autógyártók Szövetségének (ACEA) adatai szerint Kína részesedése az EU-ba irányuló elektromosautó-importból 2020-ban mintegy 15% volt. Ez jelentős növekedést jelent a néhány évvel korábbihoz képest, amikor Kína részesedése elhanyagolható volt. A kínai személygépkocsi-gyártás 2021. január–szeptemberben 14 millió darabot tett ki, ami 10,2%-os növekedést jelent az egy évvel korábbihoz képest. Kína mindeközben megőrizte pozícióját a világ legnagyobb autógyártójaként több mint 30%-os piaci részesedéssel [61].

Kereskedelmi érték (millió EUR)	**2021. január–augusztus**	**2020. január–augusztus**	**% változás 21/20**	**% részesedés 2021**
Amerikai Egyesült Államok	6016	6152	–2,2	17,6
Japán	5077	5324	–4,6	14,9
Nagy-Britannia	4884	4137	+18,1	14,3
Dél-Korea	4550	3661	+24,3	13,3
Törökország	4009	3941	+1,7	11,7
Mexikó	3145	2233	+40,9	9,2
Kína	2409	921	+161,5	7,1

Kereskedelmi érték (millió EUR)	2021. január–augusztus	2020. január–augusztus	% változás 21/20	% részesedés 2021
Marokkó	1659	1204	+37,9	4,9
Dél-afrikai Köztársaság	1240	1455	–14,7	3,6
Svájc	222	171	+29,8	0,7

6. táblázat - Az Európai Unió személygépjármű-importjának top 10 forrásországa. Forrás: saját szerkesztés az ACEA, 2021 alapján [61]

A Mercator Institute for China Studies már 2021-ben bemutatta, hogy a kínai és az európai személygépjármű-piac egyre inkább összefonódik [62]. 2022-es elemzésükben már egyértelműen állást foglalnak amellett, hogy az Európai Uniónak védelmi intézkedéseket kell bevezetnie a kínai elektromos járművek importjával szemben [63], mivel Európa vált a *made in China* elektromos járművek elsődleges célpontjává. 2021-ben Kína globális EV-exportja több mint kétszeresére emelkedett a növekvő termelési kapacitásnak köszönhetően. Ennek mintegy 40%-át Európa szívta fel, ahol a kínai EV-k már most is a teljes EV-értékesítés 10%-át teszik ki. Európa számára döntő fontosságú, hogy az EU-ba irányuló kínai EV-export nem azért nőtt, mert az autók jobbak, hanem azért, mert az európai és amerikai autógyártók áttérnek az EV-k kínai gyártására, többek között az európai piacra termelve is. A piacra jutás lazulásával párhuzamosan fokozták a beruházásokat is. Erre rengeteg példa sorolható fel, ilyen például az, hogy már a Renault Dacia Spring, valamint a Daimler BMW ikonikus Smart és Mini EV-it is Kínában fejlesztik és gyártják a globális piacokra [62].

A kínai járművekre adott európai reakció azonban nemcsak a minőségről és az árról szól, hanem politikai kérdés is. Az olyan egyéb távolkeleti OEM-anyaországok, mint például Dél-Korea, fokozott megjelenése az európai személygépjármű-piacon nem jelentett stratégiai fenyegetést az amerikai befolyásra a Csendes-óceánon, és nem voltak olyan ambíciói, mint Kínának Tajvannal kapcsolatban. Nem voltak emberi jogi vitáik, mint az ujgurok vagy más muszlimok helyzetéről folyó viták vagy a koronavírus elleni tömegtüntetések éjszakai televíziós közvetítései. Kína megjelenése az európai elektromos járművek piacán ezekből az okokból kifolyólag nemzetbiztonsági kockázatokkal is járhat. A személygépjárművek tekintetében a biztonság és a minőség mindig is kiemelt szempont volt, és ezen feltételek teljesülését ma már számos szabály írja elő az Európai Unióban. Az informatika gyors fejlődése miatt azonban ez nem mondható el feltétlenül az informatikai rendszerek biztonságáról. Ennek tudatában különösen fontos nyomon

követni a harmadik országból származó informatikai eszközök (beleértve a személygépjárművek) terjedését a piacon.

2015 óta a kínai autógyártók legalább 18 K+F- és tervezőközpontot hoztak létre Európában, hogy hozzáférjenek a piachoz, ösztönözzék az innovációt és megismerjék a helyi szabályozást. Mindez ráadásul az európai autógyártók kínai cégek általi felvásárlása mellett történik, mint például a Lotus felvásárlása a Geely által. A tisztán kínai autómárkák is egyre nagyobb számú, nagy népszerűségnek örvendő elektromos járművel törnek be az európai autópiacra, és 2022 első hét hónapjában az összes új akkumulátoros EV-regisztráció 5%-át adták Nyugat-Európában. A Schmidt Automotive Research szerint a kínai OEM-ek 200 ezer autómodellt szállítottak 2022-ben Európába. Ebből körülbelül 80-90 ezer tisztán elektromos autó, további 40 ezer pedig *plug-in hibrid* elektromos autó (PHEV), a fennmaradó 70-80 ezret pedig a hagyományos belső égésű motoros modellek teszik ki [64].

2.3 Összegzés

Az összegyűjtött adatok alapján látható, hogy a Kínai Népköztársaság hosszú távú elektromos járműgyártásra koncentráló stratégiáinak eredményeképpen az elmúlt években egyre meghatározóbb szerepet vívott ki magának a nemzetközi piacon. Bár Kína korábban is kiemelt szereplő volt a személygépjárműipar ellátási láncának tagjai között, napjainkra közvetlen érintettsége megkérdőjelezhetetlenné vált. Ez azzal jár, hogy saját gyártóinak termékei közvetlenül, az európai gyártók közreműködése nélkül jelenhetnek meg az Európai Unión belül, saját márkával, aminek következtében a járművek által gyűjtött adatok is közvetlenül juthatnak el a gyártóhoz vagy az általa kijelölt harmadik felekhez. A megfelelő stratégiák és az állam következetes támogatási programjainak köszönhetően várhatóan ezek a márkák hamarosan önállóan is képessé válhatnak jelentős mértékű piacszerzésre és a visszaszoruló európai elektromosautógyártás mellett egyre nagyobb elfogadottságra és elterjedtségre tehetnek szert.

Fontos megjegyezni továbbá, hogy a nyugati modellekhez képest jelentősen eltérő államberendezkedés miatt a gyűjtött adatok kezelésére vonatkozóan is a nyugatihoz eltérő szemléletmód vonatkozik. Ez jelentős kihívást állíthat az Európai Unió elé, hiszen a saját belső adatbiztonsági és adatvédelmi elvei nem kényszeríthetőek ki olyan mértékben, ahogyan korábban ez megoldható volt a jellemzően európai gyártóktól származó személygépjárművek esetében. Mivel a kínai piaci szereplők akkor is szoros összhangban dolgoznak az Állampárthoz kötődő megfelelő szervezeti egységekkel, ha egyébként

finanszírozásuk piaci alapú, ezért nem lehet kizárni, hogy – például egy esetleges nemzetközi konfliktus vagy piaci előnyszerzési kísérlet esetén – ez az adatgyűjtési kapacitás hátrányos helyzetbe hozza az Európai Unió államait.

3. AZ AUTÓIPARRA VONATKOZÓ SZABVÁNYOK ÉS JOGSZABÁLYOK TARTALOMELEMZÉSE, FUNKCIONÁLIS VIZSGÁLATA

Jelen fejezet az autóiparra vonatkozó különböző információbiztonsági szabványok és jogszabályok részletes vizsgálatával kívánja alátámasztani az első hipotézist, amely szerint a jelenlegi információbiztonsági szabályozási környezet nem kezeli a személygépjárművet egységes informatikai eszközként és nem fedi le megfelelő mértékben a teljes termékéletciklust. Az elemzés során áttekintem azokat a szabványokat, amelyek az autóipar kibervédelmével és adatbiztonsági követelményeivel foglalkoznak, valamint értékelem, hogy ezek a szabályozások mennyiben terjednek ki az autóipar komplex rendszereire, beleértve az autók egyes alrendszereit és beszállítói hálózatait. Ezzel célom annak bemutatása, hogy az autóipari szabványok és jogszabályok ugyan jelentős lépéseket tettek a járművek és azok alrendszereinek védelmében, azonban összességében még mindig elsősorban egy-egy alkatrészre vagy gyártói folyamatra fókuszálnak, nem pedig a járművek egységes, rendszerszintű információbiztonsági kezelésére.

Az elmúlt évek jelentős előrelépésének tekinthető a TISAX[1] és az ISO/SAE 21434[2] megjelenése, melyek specifikusan a személygépjárműipar igényeire szabott információbiztonsági szabványok. Az ISO/SAE 21434 egy termékközpontú, autóipari kibervédelemmel foglalkozó specifikus szabvány, mely meghatározza a közúti járművek elektromos és elektronikus (E/E) rendszereinek - beleértve azok alkatrészeit és kapcsolódási pontjait - koncepciójára, termékfejlesztésére, gyártására, üzemeltetésére, karbantartására és leszerelésére vonatkozó kiberbiztonsági kockázatkezelés műszaki követelményeit. Meghatározásra kerül benne egy keretrendszer, amely a kiberbiztonsági folyamatokra vonatkozó követelményeket és a kiberbiztonsági kockázatok kommunikációjának és kezelésének közös nyelvezetét tartalmazza a nemzetközi

[1] https://enx.com/en-US/TISAX
[2] https://www.iso.org/standard/70918.html

információbiztonsági szabványosítási trendeknek megfelelően. A szabvány minden sorozatgyártású közúti jármű E/E-rendszereire alkalmazandó, beleértve azok alkatrészeit és kapcsolódási pontjait, amelyek fejlesztése vagy módosítása e dokumentum kiadása után kezdődött.

Ez ígéretesen hangzik ugyan, azonban a többi szabványhoz hasonlóan, az ISO/SAE 21434 bevezetése sem kötelező, ráadásul mivel egy rendkívül fiatal, 2021-ben kiadott szabványról van szó, időbe telik az is, mire a piac befogadja és így kellő területet tud majd lefedni. A TISAX (Trusted Information Security Assessment Exchange)[3] egy olyan új biztonsági értékelési keretrendszer, amelyet az autóipar szereplői fejlesztettek ki a beszállítók biztonsági kockázatainak kezelése érdekében. Az értékelési rendszer célja, hogy a beszállítók biztonsági szintjét egységes és hatékony módon lehessen értékelni és ellenőrizni, valamint biztosítsa az autóipari vállalatok számára, hogy a beszállítóik biztonsági szintje megfelelő. A TISAX értékelési keretrendszer alapvetően az ISO/IEC 27001 információbiztonsági szabványra épül, de az autóipari beszállítók számára további biztonsági követelményeket is tartalmaz. Az értékelési folyamat során a beszállítók biztonsági szintjét egy harmadik fél értékeli és ellenőrzi, így biztosítva a független értékelést. A TISAX értékelési rendszer használata előnyös lehet a beszállítók számára, mert lehetővé teszi számukra, hogy bizonyítsák biztonsági szintjüket az autóipari partnereik számára. Emellett a TISAX értékelési keretrendszer segít a beszállítóknak abban is, hogy felmérjék saját biztonsági kockázataikat és javítsák információbiztonsági folyamataikat. [65]

A fenti szabványokon kívül érdemes még említést tenni az IEC 62443-ról[4], mely kifejezetten az ipari ellenőrzési rendszerekre vonatkozik, illetve a SAE J3061[5] szabványról, melynek lényege, hogy gyakorlati tapasztalatokat gyűjt egybe és ajánlásokat nyújt a gyártók számára az információbiztonsági folyamatok fejlesztéséhez. Az összegyűjtött jógyakorlatok legfőbb célja, hogy rugalmasak, pragmatikusak és adaptálhatók legyenek a járműiparban, valamint más területeken működő kiberfizikai járműrendszerekre nézve is (pl. kereskedelmi és katonai járművek, teherautók, buszok).

[3] https://www.tuvsud.com/en/services/auditing-and-system-certification/tisax
[4] https://www.isa.org/standards-and-publications/isa-standards/isa-iec-62443-series-of-standards
[5] https://www.sae.org/standards/content/j3061_201601

Ez az ajánlott gyakorlat azonban szintén magas szintű irányadó elveket állapít meg, tehát a konkrét megvalósításra vonatkozóan nem rögzít elvárásokat.

Ezenkívül az autógyártók az általuk gyártott autókra vonatkozó specifikus szabványokat és irányelveket is alkalmazzák (például ISO/TS 16949, amely az általános, ISO 9001 minőségbiztosítási szabvány autóipari leképezése), amelyek lehetnek nemzetközi vagy helyi szintűek. Az Európai Unióban az autókra vonatkozó szabványokat az Európai Bizottság, míg az Egyesült Államokban a Nemzeti Autópálya-biztonsági Hivatal (NHTSA) határozza meg, így attól függően is eltérés tapasztalható a követelmények között, hogy a világ melyik pontját vizsgáljuk. Az Európai Uniót tekintve az elmúlt években egyre nagyobb hangsúlyt kapott a GDPR és ennek hatására más területek is nagyobb hangsúlyt kezdtek fektetni az adatvédelemre. Ennek köszönhetően a felsorolt szabványokban is egyre nagyobb súllyal jelent meg az adatvádelem kérdésköre. Ezzel együtt is elmondható azonban, hogy a szabályozások közül egyedül a GDPR fókuszál kifejezetten a fogyasztók adataira és az adatáramlás átláthatóságára. Jelen tanulmánynak nem célja teljeskörűen bemutatni a GDPR-al kapcsolatos problémákat, de információbiztonsági kontextusban is érdemes kiemelni, hogy a nemzetközi szakirodalom számos olyan példát szolgáltat, melyek alátámasztják, hogy a rendeletet szükséges fejleszteni. [66], [67], [68]

Szintén fontos megjegyezni, hogy a hálózati kommunikáció miatt a tanulmány témájához kapcsolódnak a különböző felhőszolgáltatásokra vonatkozó szabályozások, illetve egy sor ipari eszközökre vonatkozó szabályozás is, ám ezekre jelen kutatás terjedelmi okok miatt szintén nem tér ki.

3.1 Főbb személygépjárműipart érintő jogszabályok és szabványok bemutatása

A fenti általános áttekintés után listába gyűjtöttem azokat a szabályozásokat, melyek kifejezetten a személygépjárműiparra vonatkoznak és kiberbiztonsági fókuszúak vagy legalább is van olyan elemük, mely az adatbiztonságra fókuszál. A listából kihagytam az általános, iparra és gyártásra vonatkozó szabályozásokat. Elemzésemben ennek megfelelően a továbbiakban az alábbi jogszabályokat és szabványokat veszem figyelembe:

- ISO/SAE 21434 – Road Vehicles Cybersecurity Engineering

- UNECE WP.29 – R155 and R156
- ISO 26262 – Functional Safety for Road Vehicles
- ISO/IEC 27001 – Information Security Management
- NIST Cybersecurity Framework
- AUTOSAR Adaptive Platform
- ISO/IEC 15408 – Common Criteria
- ISO 24089 – Software Update Engineering
- GDPR – General Data Protection Regulation
- CISPR 25 – Vehicle EMC
- TISAX – Trusted Information Security Assessment Exchange
- SAE J3061 – Cybersecurity Guidebook
- ASPICE – Automotive SPICE
- ISO 21448 – Safety of the Intended Functionality (SOTIF)
- NHTSA Cybersecurity Guidelines

Az ENSZ három új szabvány bevezetésével igyekszik megoldást találni a kihívásokra. Az UNECE hivatalos weboldalán található, a járműipari kibervédelem helyzetéről szóló összefoglaló három jelentős ENSZ-járműszabályozásra fókuszál [69], amelyek már hatályba léptek. Az első szabályozás az ENSZ 155. szabályozása (R155), amely egységes rendelkezéseket tartalmaz a járművek típusjóváhagyásával kapcsolatban a kiberbiztonság és a kiberbiztonsági menedzsmentrendszer (CSMS) tekintetében. A második szabályozás az ENSZ 156. szabályozása (R156), amely követelményeket állapít meg a biztonságra vonatkozóan, különös hangsúlyt fektetve a szoftverfrissítésekre. A harmadik szabályozás az UNECE WP.29 (United Nations Economic Commission for Europe) keretében megjelent szabályozás, amely a járművek kiberbiztonságának és szoftverfrissítéseinek területén szabályozó fórumot nyújt. Ezen szabályozások célja, hogy biztosítsák az autók biztonságát, és meghatározzák az autóipari kiberbiztonság keretrendszerét a piacra kerülő személygépjárműtípusokra nézve.

Az Európai Unióban folyamatosan folynak viták az eseménynapló-berendezések kötelező telepítéséről, amely téma korábban Nagy-Britanniában ellenállást váltott ki, mivel a szabadság és a választás szabadságának elveivel szembeni lépés lenne. Az igazság valójában az, hogy ilyen „feketedobozok” már hosszabb ideje léteznek az autókban. Ezek az eszközök eredetileg főként a légzsákok információforrásaként szolgáltak azzal a céllal,

hogy a megfelelő körülmények fennállása idején aktiválják azokat. Ennek eredményeként az egység fejlődött, és egyre több információt is kezdett gyűjteni. Napjainkban nemcsak a jármű sebességét és helyzetét tudjuk meg a benne található adatokhoz hozzáférve, hanem például a pedálok helyzetét vagy a kormánykerék pozícióját is [70].

Látható tehát, hogy már elindult az a fajta változás, amely a szigorúbb szabályozási környezet kialakításának irányába mutat. A személygépjármű azonban komplex termék, a beszállítókat pedig – elvileg az átfogó szabályozások, mint amilyen az ISO 27001 is – kötelezik arra, hogy a gyártóhoz hasonlóan bevezessék magukra vonatkozóan is az ott alkalmazott szabványokat, ám a gyakorlatban sok esetben egy végeláthatatlan folyamatba torkollik ez a kezdeményezés. Mivel az informatikai rendszerekre más specifikus ágazati szabványok vonatkoznak, ez a rendszer alapjaiban tökéletlen. Bár az ISO 27001 lehetőséget biztosít az alaposságra, nagyban függ a humán és anyagi erőforrásoktól, hogy milyen mélységig, hogyan, milyen eszközökkel alkalmazza a szabványt, és milyen problémákat próbál inkább kerülő utas megoldásokkal orvosolni a vállalat.

3.2 A főbb személygépjárműipart érintő szabványok és jogszabályok vizsgálata különböző szempontok alapján

Az előző fejezetben láthattuk, hogy a járműipart érintő jogszabályok és szabványok tematika szempontjából jól kiegészítik egymást – még egy részük funkcionális szemléletű, egy másik részük az adatvédelemre vagy éppen a fenyegetésekre fókuszál. Problémát jelent azonban, hogy ezeknek a szabályoknak az érvényesítése csak a legritkább esetekben valósul meg egyszerre, hiszen nagy részük nem kötelező jellegű és az alkalmazás felügyeletére sincsen kijelölve hivatalos szerv.

Szabvány/Jogszabály	Elterjedtség	Kötelező?	Érintettek	Felügyelet	Szankciók
ISO/SAE 21434 – Road Vehicles Cybersecurity Engineering	Széles körben alkalmazott, de nem kötelező.	Nem kötelező	Autógyártók, beszállítók	Nincs hivatalos felügyelet	Nincsenek hivatalos szankciók
UNECE WP.29 – R155 and R156	Kiterjedt az EU-ban és egyéb UNECE-tagországokban.	Igen, kötelező EU-ban és UNECE-tagországokban	Autógyártók, szoftver- és hardverbeszállítók	Nemzeti közlekedési hatóságok	Típusjóváhagyás megtagadása, forgalmazás kizárása

Szabvány/Jogszabály	Elterjedtség	Kötelező?	Érintettek	Felügyelet	Szankciók
ISO 26262 – Functional Safety for Road Vehicles	Széles körben alkalmazott, különösen biztonságkritikus rendszerekhez.	Nem mindenhol kötelező	Autógyártók, beszállítók, különösen biztonságkritikus rendszerekkel foglalkozók	Nincs közvetlen hatósági felügyelet	Az OEM megtagadhatja a beszállítótól a termékek átvételét
ISO/IEC 27001 – Information Security Management	Általános ipari szabvány, széles körben alkalmazott a biztonsági rendszerekre.	Nem kötelező az autóiparban	Autógyártók, beszállítók, IT cégek	Szabvány szerinti auditálás	Tanúsítvány hiánya szerződésbeli következményekhez vezethet
NIST Cybersecurity Framework	Elsősorban az USA-ban alkalmazott, nemzetközileg is elismert.	Nem kötelező	Elsősorban amerikai cégek, globálisan is alkalmazható	Nincs közvetlen hatósági felügyelet	Nincsenek jogi szankciók, de reputációs és gazdasági hátrányok merülhetnek fel
AUTOSAR Adaptive Platform	Széles körben alkalmazott az autonóm és modern járműveknél.	Nem kötelező	Szoftver- és hardverbeszállítók, autógyártók	Az AUTOSAR konzorcium felügyeli	Nincsenek hivatalos szankciók
ISO/IEC 15408 – Common Criteria	Globálisan elismert szabvány biztonságkritikus rendszerekhez.	Nem kötelező	Autógyártók, beszállítók, beépített rendszerekkel foglalkozók	Nemzeti kormányok által kiadott tanúsítványok	Tanúsítvány nélkül piacvesztés következhet
ISO 24089 – Software Update Engineering	Újabb szabvány, terjedőben.	Nem kötelező	Autógyártók, szoftverfejlesztők, beszállítók	Nincs közvetlen felügyelet	Az OEM-ek megkövetelhetik, de nincs jogi szankció
GDPR – General Data Protection Regulation	Kötelező az EU-ban minden, személyes adatokat kezelő szervezet számára.	Igen, kötelező az EU-ban	Autógyártók, forgalmazók, szoftverfejlesztők	EU tagállami adatvédelmi hatóságok	Pénzbírságok (akár a globális éves forgalom 4%-áig)
CISPR 25 – Vehicle EMC	Széles körben alkalmazott az elektromos rendszerekre vonatkozóan.	Általában kötelező	Autógyártók, elektronikai beszállítók	Nemzeti hatóságok	A forgalmazási engedély megtagadása
TISAX – Trusted Information Security Assessment Exchange	Európában széles körben elterjedt az autóipari szereplők között.	Nem kötelező jogilag	Autógyártók, beszállítók	ENX Association által kezelt auditálás	Beszállítói szerződésből való kizárás, ha nem felel meg
SAE J3061 – Cybersecurity Guidebook	Széles körben ismert és alkalmazott a kiber-fizikai rendszerek fejlesztésében.	Nem kötelező	Autógyártók, szoftver- és hardverbeszállítók	Nincs hivatalos felügyelet	Nincsenek jogi szankciók, de versenyhátrányt okozhat

Szabvány/Jogszabály	Elterjedtség	Kötelező?	Érintettek	Felügyelet	Szankciók
ASPICE – Automotive SPICE	Széles körben alkalmazott szoftverfejlesztési értékelési modell.	Nem kötelező jogilag	Autógyártók, szoftverfejlesztők, beszállítók	Az autógyártók auditálhatják a beszállítókat	Kizárhatják a beszállítókat, ha nem felel meg a követelményeknek
ISO 21448 – Safety of the Intended Functionality (SOTIF)	Növekvő jelentőségű az autonóm járművek fejlesztésében.	Nem kötelező	Autógyártók, beszállítók	Nincs hivatalos felügyelet	Nincsenek közvetlen szankciók
NHTSA Cybersecurity Guidelines	Az USA-ban elterjedt ajánlás formájában létezik, nem jogszabály.	Nem kötelező	Autógyártók, beszállítók, főként az USA-ban	Az NHTSA (USA Nemzeti Közúti Közlekedésbiztonsági Hatósága)	Nincsenek hivatalos szankciók, de reputációs kockázatok lehetnek

7. táblázat - A szabályozási környezet értékelése - Átfogó vizsgálat

Problémát okoz az is, hogy a felsorolt szabványok nagy része folyamatközpontú, és a gyártó adatainak védelmére fókuszál. Ezek között kivételt képez az ISO 21434 szabvány, amely kifejezetten egy-egy alkatrész vizsgálatát célozza. Ennek hiányossága azonban, hogy a személygépjármű nem minden alkatrészére terjed ki, hanem csak azokra, amelyekre a gyártó valami miatt fontosnak tartja elvégeztetni.

A kiberbiztonságra vonatkozó fő kutatások során a biztonsági fenyegetések és támadások széles körű irodalma jött létre, azonban ezek alig tesznek említést a járműipar kiberbiztonsági tanúsításáról és auditálásáról. Az egyik fő ok az, hogy az önvezető járművek egy feltörekvő többszereplős piacot képviselnek, amelyet a kapcsolódó technológiák gyors fejlődése és innovációja jellemez. Ennek eredményeként a kiberbiztonsággal nem foglalkoztak kellő alapossággal az előző járműipari szabványokban, például az ISO 26262-es szabványban, amely nem fektetett le alapokat a szektor harmonizált fejlesztéséhez. Az első gyakorlati alapú specifikus autóipari kiberbiztonsági szabvány, a SAE J3061 szabvány például csak 2016-ban jelent meg [71].

A fejezet eredményei alapján megállapítható, hogy az autóipari szabályozási környezet valóban nem biztosít egységes információbiztonsági megközelítést a személygépjárművekre mint integrált informatikai eszközökre. Az elemzés rávilágított arra, hogy bár több új szabvány – például az ISO/SAE 21434 és a TISAX – bevezetésével az autóipar igyekszik alkalmazkodni a kiberbiztonsági kihívásokhoz, ezek a szabványok főként „önkéntes” iránymutatásokat kínálnak avagy a piaci vonzerőre alapozzák a betartást, és elsősorban a gyártókra, illetve specifikus alrendszerekre vonatkozó követelményekre összpontosítanak. Így a fejezet megállapításai alátámasztják azt a

feltételezést, hogy a jelenlegi jogszabályi keretek nem fedik le teljeskörűen a személygépjárműveket egységes informatikai eszközként, ami tovább növeli az átfogó és kötelező érvényű szabályozások szükségességét.

3.3 Keretalapú tartalomelemzés (Framework Analysis)

A fenti vizsgálat elvégzéséből fakad az az igény, hogy a szabványokat és jogszabályokat tartalmuk alapján halmazokba soroljuk, hogy elkülöníthetőek legyenek azok, amelyek a leginkább illeszkednek az értekezésben feltárt igényekhez. A szabványok és jogszabályok megismerése és értelmezése nem mindig magától értetődő feladat, így ez a fajta tartalomelemzés sem teljeskörű, ebben a fejezetben pusztán csak a vizsgálathoz legszükségesebb szabályozások kiválogatásához használom. Az egyes szabványok különböző, de mégis egymáshoz kapcsolódó célokat szolgálnak az autóipari rendszerek biztonsága, funkcionalitása és adatvédelme szempontjából, így kialakíthatóak köztük témakör szerinti csoportok.

3.3.1 Tematikus keret kialakítása

A tartalmi elemzés elején különböző témaköröket határoztam meg, melyekbe a tartalmuk alapján besoroltam a szabályozásokat. A továbbiakban röviden ezen főbb témakörök mentén vizsgálom meg a szabványokat:

- **Kiberbiztonság:** ISO/SAE 21434, NIST Cybersecurity Framework, UNECE WP.29, SAE J3061, és NHTSA Cybersecurity Guidelines.
- **Funkcionális biztonság és szoftverfrissítések:** ISO 26262, ISO 21448, ISO 24089.
- **Információbiztonság:** ISO/IEC 27001, GDPR, TISAX, ISO/IEC 15408.
- **Automatizált szoftverfejlesztési gyakorlatok:** AUTOSAR Adaptive Platform, ASPICE.
- **Elektronikai zavarvédelem (EMC):** CISPR 25.

3.3.2 Indexelés

Az indexelés során a fenti témakörök alapján az egyes szabványok főbb jellemzőit és célkitűzéseit különítem el:

Szabvány/Jogszabály	Fő célja/területe	Kategória	Főbb követelmények vagy irányelvek
ISO/SAE 21434	Autóipari kiberbiztonsági mérnökség	Kiberbiztonság	Fenyegetés-elemzés, kockázatkezelés, biztonsági intézkedések
UNECE WP.29 – R155, R156	Járművek kiberbiztonsága és szoftverfrissítések	Kiberbiztonság és frissítés	Kiberbiztonsági követelmények, szoftverfrissítés menedzsment
ISO 26262	Funkcionális biztonság	Funkcionális biztonság	Funkcionális biztonsági követelmények, ASIL szintek
ISO/IEC 27001	Információbiztonság-menedzsment	Információbiztonság	Információvédelmi irányelvek, kockázatkezelési keret
NIST Cybersecurity Framework	Általános kiberbiztonsági keretrendszer	Kiberbiztonság	Azonosítás, védelem, detektálás, válaszadás és helyreállítás
AUTOSAR Adaptive Platform	Automatizált jármű szoftverek platformja	Automatizálás	Integrált architektúra, kommunikációs protokollok
ISO/IEC 15408 (Common Criteria)	Információs rendszerek biztonsági követelményei	Információbiztonság	Biztonsági funkciók követelményei, értékelési szintek
ISO 24089	Szoftverfrissítések kezelése	Funkcionális biztonság és frissítés	Szoftveréletciklus menedzsment, frissítési eljárások
GDPR	Adatvédelem	Információbiztonság	Adatkezelési elvek, jogok, adatbiztonsági követelmények
CISPR 25	Elektronikai zavarvédelem (EMC)	EMC	EMC szabványok, interferenciavédelem
TISAX	Biztonságértékelés (autóipari ellátási lánc)	Információbiztonság	Adatvédelmi auditálás, ellátási lánc biztonság
SAE J3061	Kiberbiztonsági útmutató autóipar számára	Kiberbiztonság	Kockázatelemzés, válaszintézkedések, vészhelyzeti eljárások
ASPICE	Autóipari szoftverfejlesztési folyamatok	Automatizálás	Minőségi szintek, fejlesztési ciklus, ellenőrzési folyamatok

Szabvány/Jogszabály	Fő célja/területe	Kategória	Főbb követelmények vagy irányelvek
ISO 21448	A tervezett funkcionalitás biztonsága	Funkcionális biztonság	Megfelelőségi elemzés, hibakezelési eljárások
NHTSA Cybersecurity Guidelines	Kiberbiztonsági ajánlások az autóipar számára	Kiberbiztonság	Járművek kiberbiztonsági eljárásai

8. táblázat - A szabályozási környezet értékelése - Indexelés

3.3.3 Leképezés

A különböző szabványokat és jogszabályokat összekapcsolva, láthatóvá válik, hogy a kiberbiztonsági és információbiztonsági szabványok hangsúlyosak, különösen a modern, hálózatba kapcsolt járművek esetében. Az ASPICE és AUTOSAR Adaptive Platform például különösen fontos a szoftverfejlesztési folyamatoknál, míg a GDPR és TISAX az adatvédelem és biztonság biztosítása érdekében kritikus az ellátási lánc és adatkezelési rendszerek számára. Az értekezés hipotéziseinek vizsgálatához azonban ezek elemzése kevésbé járul hozzá, mivel vagy az alanyuk (tématerületeik) vagy pedig megközelítésük (főbb követelményeik és irányelveik) nem az általan vizsgált témakörökre irányulnak.

3.3.4 Értelmezés

Az elemzés eredményeként megállapítható, hogy ezen szabványok elméleti síkon egymást kiegészítve járulnak hozzá a modern autóipar biztonságos működéséhez. A kiberbiztonsági (ISO/SAE 21434, UNECE WP.29), információbiztonsági (ISO/IEC 27001, GDPR) és funkcionális biztonsági (ISO 26262, ISO 21448) szabványok megfelelő alkalmazás esetén szinergiában működhetnek, hogy a járművek megbízhatósága, adatainak védelme és az utasok biztonsága garantált legyen. Az AUTOSAR Adaptive Platform és ASPICE a szoftverfejlesztési folyamatokat támogatják, míg a CISPR 25 az elektronikai eszközök zavarvédelmét szolgálja.

Az ISO 24089 új frissítési mérnökségi szabvány fontos a jövőbeni szoftverfrissítések kezelésében, biztosítva, hogy az új szoftverek kompatibilisek és biztonságosak maradjanak a jármű teljes életciklusa alatt. Nem életszerű azonban, hogy ezek a szabványok és szabályozások valóban egyszerre teljesüljenek, hiszen általában már egy szabványnak való megfelelés is nagy erőforrásigénnyel jár a gyártók és az ellátási lánc számára.

3.4 Tematikus elemzés (Thematic Analysis)

Braun és Clarke (2006) [70] szerint a tematikus elemzés rugalmasságot biztosít a kvalitatív adatelemzés során, különösen, ha az elemzett szövegben visszatérő témák feltárása a cél. A tematikus elemzés (Thematic Analysis) módszertana alapján részletesebb betekintést adhatunk az autóipari és információbiztonsági szabványok és irányelvek struktúrájába. A tematikus elemzés során a szakirodalom alapján hat lépést követek: ismerkedés az adatokkal, kódolás, kezdeti témák azonosítása, témák felülvizsgálata, témák meghatározása és elnevezése, valamint az eredmények összeállítása. Célom, hogy a fent elvégzett elemzési eredményekhez képest egy másik aspektusból is megvizsgálhassam a felsorolt szabályozásokat, majd az eredmények összevetése alapján biztonsággal zárhassam ki azokat, amelyek nem segítik a hipotézisek vizsgálatát.

3.4.1 Ismerkedés az adatokkal

Az első lépésben részletesen áttekintettem a szabványokat, és azonosítottam a főbb célokat és kategóriákat, amelyeket az egyes dokumentumok lefednek. Ez az alapos áttekintés lehetővé tette, hogy jobban megértsem, hogyan illeszkednek ezek a szabványok az autóipari és kiberbiztonsági kontextusba.

3.4.2 Kódolás

Az egyes szabványokra vonatkozó kódokat a következő kulcstémák mentén hoztam létre a tartalmuk vizsgálata után:

- **Kiberbiztonság:** Fenyegetéskezelés, kockázatelemzés, biztonsági folyamatok és intézkedések (pl. ISO/SAE 21434, NIST Cybersecurity Framework, SAE J3061).
- **Adatvédelem és adatbiztonság:** Adatvédelmi jogok, adatbiztonsági protokollok és auditálási eljárások (pl. GDPR, TISAX).
- **Funkcionális biztonság:** Hibakezelés, ASIL szintek, szoftverfrissítési eljárások és a tervezett funkcionalitás biztonsága (pl. ISO 26262, ISO 24089, ISO 21448).
- **Szoftverfejlesztési és automatizálási gyakorlatok:** Fejlesztési protokollok, integráció és minőségbiztosítás (pl. AUTOSAR Adaptive Platform, ASPICE).
- **Elektronikai zavarvédelem (EMC):** Elektromágneses kompatibilitási követelmények (pl. CISPR 25).

3.4.3 Kezdeti témák azonosítása

A kódok alapján öt fő témát emeltem ki, amelyek a következő kategóriák köré csoportosulnak:

- Kiberbiztonsági védelmi rendszerek és eljárások: Az autóipari szabványok közül több (ISO/SAE 21434, SAE J3061, UNECE WP.29) a kiberbiztonsági veszélyek kezelése, a fenyegetésmodellezés és a kockázatkezelés fontosságát hangsúlyozzák.
- Adatvédelem és adatkezelési protokollok: A GDPR és TISAX szigorú adatvédelmi elvárásokat támaszt, biztosítva, hogy a felhasználói adatok biztonságosak legyenek az autóipari ellátási láncban.
- Funkcionális biztonsági intézkedések és frissítési eljárások: Az ISO 26262, ISO 24089 és ISO 21448 szabványok a funkcionális biztonságra, szoftverfrissítésekre és a meghibásodások kezelésére összpontosítanak.
- Szoftverfejlesztés és automatizálási keretek: Az AUTOSAR Adaptive Platform és ASPICE szabványok a járműipari szoftverfejlesztés folyamatosságát és hatékonyságát célozzák.
- Elektronikai zavarvédelem (EMC): A CISPR 25 szabvány kifejezetten a járműelektronikai rendszerek zavartűrésére és EMC szabványokra fókuszál.

3.4.4 Témák felülvizsgálata

A témákat újra áttekintve ellenőriztem, hogy minden kód illeszkedik-e a megfelelő témához. E folyamat során bizonyos átfedések és kapcsolódások is előkerültek, különösen a kiberbiztonság és adatvédelem, valamint a funkcionális biztonság és frissítési eljárások között, amelyek sok szempontból összefonódnak.

3.4.5 Témák meghatározása és elnevezése

A témák áttekintése után a következő elnevezésekkel határoztam meg őket:

- Kiberbiztonság és fenyegetéskezelés: A járművek védelmére szolgáló szabványok, amelyek a kockázatelemzés, fenyegetésmodellezés és a biztonsági incidensek kezelése köré összpontosítanak.
- Adatvédelmi és adatbiztonsági szabályozások: Az adatkezelés, adatbiztonság és adatvédelmi jogok biztosítása, különösen a GDPR és TISAX keretein belül.
- Funkcionális biztonság és frissítési folyamatok: A biztonságos járműműködés biztosítása, valamint a frissítési és hibakezelési eljárások.

- Szoftverfejlesztési és minőségbiztosítási keretrendszerek: A szoftverfejlesztési folyamatok, amelyek az autóipari környezetben integrálják a minőségellenőrzést és fejlesztési protokollokat.
- Elektronikai zavarvédelmi irányelvek: Elektromágneses interferenciák csökkentése és zavarvédelem az autóipari elektronikai rendszerekben.

3.4.6 Eredmények összeállítása

A tematikus elemzés alapján a következő megállapításokat lehet tenni:

Az autóipari szabványok, mint az ISO/SAE 21434 és UNECE WP.29, kulcsfontosságúak a kiberbiztonsági eljárások biztosításában, segítve a gyártókat a fenyegetések elleni védekezésben. A GDPR és TISAX adatvédelmi követelményei kiemelkedő fontosságúak a felhasználói adatok védelme és az autóipari beszállítói láncban történő adatáramlás ellenőrzése szempontjából. Az ISO 26262 és ISO 24089 szabványok meghatározóak a járművek biztonságos működéséhez, biztosítva, hogy a funkcionális biztonsági intézkedések és frissítési eljárások jól dokumentáltak és következetesek legyenek. Az AUTOSAR és ASPICE a szoftverek megbízhatóságát és hatékony integrációját segítik az autóipari rendszerekben, különös tekintettel az adaptív rendszerekre. A CISPR 25 szabvány segít az autóipari elektronikai rendszerek zavartűrő képességének növelésében, csökkentve az elektromágneses interferenciát és biztosítva a zavartalan működést.

3.5 Összegzés

A tartalmi elemzés alapján látható, hogy azok a szabályozások, amelyek egyszerre helyezik középpontba a személygépjárműipart és a kiberbiztonságot, illetve nem pusztán a gyártási folyamatokkal, hanem a személygépjárművel mint termékkel is foglalkoznak, az UNECE WP.29 – R155, R156, az ISO 26262 és az ISO/SAE 21434. Mivel az UNECE WP.29 – R155 és R156 kifejezetten a típusjóváhagyási folyamatra összpontosít, az általános, visszamenőleg is alkalmazandó szabványokkal ellentétben kevésbé releváns.

Az ISO27001 szabvány – bár nem iparágspecifikus és az általános folyamatokra fókuszál – illeszkedik a vizsgálati körbe, mivel elterjedtsége és ismertsége nagy és kifejezetten az információbiztonsági irányítási rendszer kialakítása a célja. Elvárja továbbá, hogy ez a rendszer a szervezet működésének szerves részeként valósuljon meg, lefedve minden folyamatot.

A vizsgálat folytatásához tehát főként az ISO 27001, az ISO/SAE 21434, és az ISO 26262 szabványokra fókuszálok, hiszen a szakirodalom elemzése alapján ezek követelményrendszere áll legközelebb a megfogalmazott igényekhez.

4. KÉRDŐÍVES KUTATÁS – A FELHASZNÁLÓK PERCEPCIÓI AZ OKOS JÁRMŰVEK KAPCSÁN

Ez a kérdőíves kutatás arra irányul, hogy a válaszadók személygépjárművekkel kapcsolatos adatkezelési tudatosságát és tájékozottságát felmérje, ezzel alátámasztva a H3 hipotézist, miszerint a tulajdonosok nem kapnak elegendő tájékoztatást a járműveik által végzett adattovábbításról, így nincsenek tisztában a személyes adataik kezelésével kapcsolatos kockázatokkal. A kérdőív felépítésében nagy hangsúlyt kapott az adatküldési funkciókkal kapcsolatos tudás szintjének felmérése, például hogy a válaszadók tisztában vannak-e azzal, hogy járművük képes-e internetkapcsolatra, illetve hogy továbbít-e adatokat a gyártónak vagy harmadik félnek. További kérdések vonatkoznak arra, hogy a válaszadók szerint fontos-e a tájékoztatás az adatküldésről, illetve kaptak-e valaha ilyen információt, például adatvédelmi tájékoztató, szervizelési tanácsadás vagy gyártói kommunikáció formájában. E kérdések azt vizsgálják, hogy a válaszadók mennyire ismerik autójuk adatkezelési gyakorlatát és annak lehetséges biztonsági és adatvédelmi kockázatait, valamint milyen mértékben érzékelik ennek jelentőségét.

A kérdőíves kutatás módszertani alapját a kvalitatív és kvantitatív elemeket ötvöző, vegyes módszertan képezi [72], [73], [74], [75], amely lehetőséget biztosít a kérdések egy részének strukturált, zárt formában történő megválaszolására, miközben másik részük esetén nyitottabb válaszlehetőségeket kínál, amelyek alapján részletesebben megismerhető az alanyok gondolati világa. Így a válaszok számszerűsíthetők és statisztikai módszerekkel elemezhetők, miközben a nyílt végű kérdések a válaszadók szubjektív véleményét és személyes értékelését is felszínre hozzák, lehetőséget teremtve a kvalitatív elemzésre. A kérdőív így egyszerre gyűjt pontosan mérhető adatokat és nyújt betekintést a válaszadók attitűdjeibe, félelmeibe és információigényébe. A kérdőív összeállításakor különös figyelmet fordítottunk a kérdésfeltevések egyértelműségére és az elfogultság minimalizálására, hogy a válaszok hitelesen tükrözzék a válaszadók ismeretszintjét és attitűdjeit [76]. Ez a módszertani megközelítés lehetőséget ad arra, hogy az eredmények részletes és árnyalt képet nyújtsanak arról, hogy a felhasználók mennyire

tájékozottak a személygépjárművek adatkezelési gyakorlataival kapcsolatban, és milyen mértékben vannak tudatában az adataik kezeléséből fakadó kockázatoknak.

4.1 Általános módszertan

A kérdőíves kutatás egy 30 fős magyar pilot mintán kezdődött. Ebben a szakaszban a válaszadók a nyitott, kifejtős válaszokra adott válaszait elemeztem annak érdekében, hogy az egyes kérdések megfelelő mélységű információt szolgáltassanak a kutatási cél elérése érdekében. A kérdőív eredeti, magyar verziójának finomhangolása (pl. a szabadszöveges inputok alapján több zárt választási lehetőséges kérdés meghatározása) után a kérdéseket angol nyelvre lefordítottam, így lehetővé téve a kutatás nemzetközi kiterjesztését is.

A kérdőívben feltett kérdések a következő kategóriákra oszthatók:

Alapvető Demográfiai Információk:

- Az életkor és a származási ország rögzítése.

Gépjárműtulajdonosi Tapasztalatok és Preferenciák:

- Kérdések a személygépjármű tulajdonlására vonatkozóan (pl. „Jelenleg van személygépjárműve?” vagy „Milyen márkájú autót birtokolt legutóbb?”).
- A válaszadó és családtagjai tulajdonában lévő autók száma.

Okosautó-technológiával Kapcsolatos Tudatosság:

- A válaszadók tudatosságának felmérése, például, hogy tudják-e, hogy autójuk képes csatlakozni az internethez, vagy rendelkeznek-e okosautóval.

Adattovábbítás és Adatvédelem Tudatossága:

- Kérdések arra vonatkozóan, hogy a válaszadók tudják-e, hogy autójuk adatokat továbbít-e a gyártónak vagy harmadik félnek, és hogy kaptak-e erről tájékoztatást.

Adatvédelem és Kockázatérzékelés:

- Nyitott kérdések a potenciális kockázatokkal kapcsolatban, például hogy miért tartják problémásnak, ha a jármű felhasználói tudta nélkül adatokat továbbít.

Autóválasztási Preferenciák:

- Preferenciák a gépjárművek származási országa tekintetében (pl. melyik országból választana vagy nem választana autót, és miért).

4.1.1 Célcsoport

A kutatás célcsoportja széleskörű volt, mivel a kérdések közül több általános véleményre irányult, mint például a jármű származási országának preferenciája vagy az adattovábbítási kockázatokkal kapcsolatos gondolatok. Azonban bizonyos kérdések csak olyan válaszadókra vonatkoztak, akik rendelkeznek vagy rendelkeztek személygépjárművel, például hogy kaptak-e tájékoztatást az autójuk által végzett adattovábbításról. A két csoport elkülönítését ellenőrző kérdés, illetve a kötött listás válaszok között specifikus válaszok elhelyezésével tettem lehetővé (tehát minden személygépjárműtulajdonosoknak szóló kérdés esetében szerepelt a válaszok között a „nem rendelkezem saját személygépjárművel” válasz).

4.1.2 Mintavételi Módszer és Terjesztés

A kérdőív terjesztése főként egyetemi Facebook csoportokon, valamint tematikus autós online fórumokon és csoportokon keresztül történt. Emellett nemzetközi ismeretségi körben, valamint nemzetközi egyetemi hallgatók körében is megosztottam, így összesen 289 választ gyűjtve.

A célcsoport kiválasztása során különböző kulturális hátterű célországokat bevonására törekedtem. Az elektomos személygépjárművek elterjedésében Norvégia vezető helye a világon mégkérdőjelezhetetlen. Az új autó eladások tekintetében az elektromos autók aránya Norvégiában évek óta 90% feletti, ez az arány az okosautók tekintetében közel 100 százalékos. [6] A teljes forgalomban lévő autóparkot figyelembe véve az elektromos autók száma egymillióhoz közelít, amely több mint egyharmada a teljes forgalomban lévő autóparknak (kb. 2.5 millió autó). Norvégia emiatt megfelelőnek bizonyult a felmérés mintavételezésére, hiszen rendkívül sok tapasztalat áll rendelkezésre az internetre kapcsolt személygépjárművekkel kapcsolatban, illetve a célcsoport elérését ebben az országban megkönnyítette a személyes akadémiai kapcsolat is. Mivel közel minden második személygépjármű okosautónak tekinthető, a norvég hallgatók által adott válaszokat különösen értékes adatforrásnak tartom.

Az internetkapcsolatra képes személygépjárművekkel kapcsolatos releváns tapasztalatok összegyűjtése mellett ugyanakkor arra is kíváncsi voltam, hogy ahol még viszonylag

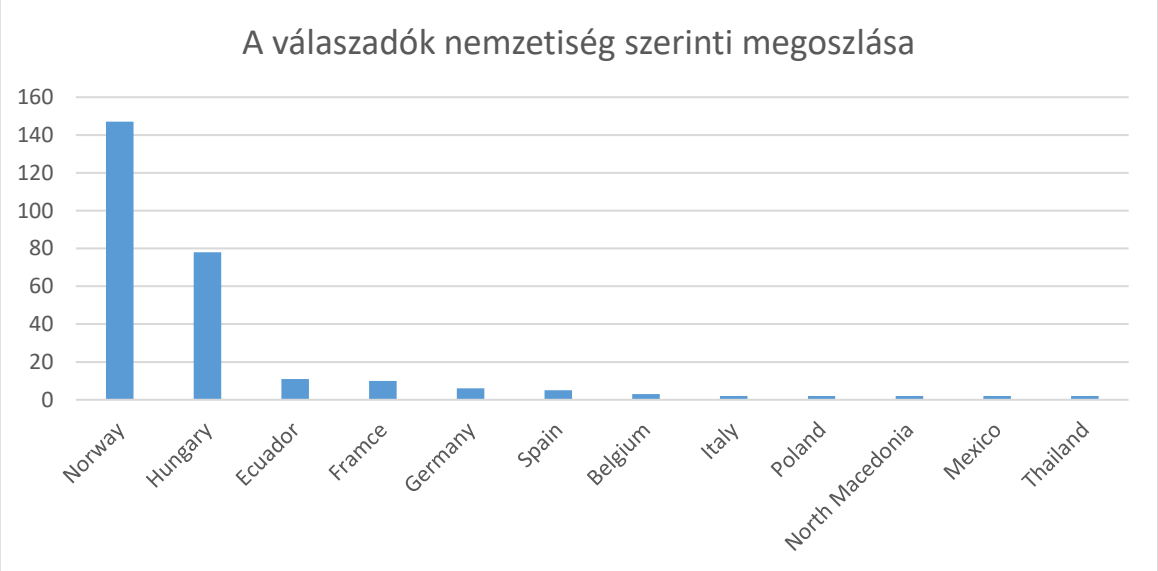
[6] https://elbilstatistikk.no/

kevés ismeret áll rendelkezésre az okosautókkal kapcsolatban, milyen információk gyűlnek össze. Erre a célra Magyarország vizsgálatát megfelelőnek tartom, bár ez a közeljövőben feltehetően változni fog tekintettel a közelmúltbeli beruházások kiterjedtségére. A kutatás során szerencsés egybeesés volt, hogy német és francia válaszadók válaszai is viszonylag magas számban álltak rendelkezésre. Németország a világ egyik vezető autógyártója, ugyanakkor jelenleg éppen az elektromos okosautók terjedése miatt szembesül jelentős kihívásokkal. Franciaország vezető autógyártó nemzet Európában, így ezek válaszok szintén érdekesek.

Származási ország	Válasz (db)
Norvégia	147
Magyarország	78
Ecuador	11
Franciaország	10
Németország	6
Spanyolország	5
Belgium	3

9. táblázat - Top 7 nemzet megjelenése a mintában:

Összesen 29 országból érkezett válasz, köztük pl. Vietnámból, Mongóliából, Ukrajnából, Pakisztánból, a balti államokból. A válaszadók nemzetiség szerinti megosztását az alábbi ábra szemlélteti:



3. ábra - A kérdőíves kutatás válaszadóinak nemzetiség szerinti megoszlása

4.1.3 A kérdőív megbízhatóságának vizsgálata

A kérdőíves adatok értékelésének kontextusában a belső konzisztencia kulcsfontosságú mutató, amely betekintést nyújt abba, hogy egy kérdéscsoport mennyire képes egyetlen mögöttes gondolati konstrukció mérésére. Az elemzés során a teljes kérdőív olyan kérdéseire fókuszáltam, amelyek a résztvevők okosautó-funkciókkal, különösen az adatmegosztással és adatbiztonsággal kapcsolatos tudatosságát, ismereteit és véleményét vizsgálták.

Az ellenőrzésből azonban kizártam a nyitott kérdéseket, hiszen ezek maximum szubjektív kategóriák kialakítása után alkalmasak arra, hogy a belső összefüggéseket mérjük – azonban az objektivitás szempontjából ez már eleve egy torzított adatforrás lett volna. A fennmaradó eldöntendő kérdések, melyekre a válaszadók kötött válaszokat adhattak, azonban alkalmasak arra, hogy következtetést vonjunk le a kérdőív eredményeinek egészére nézve.

Az elemzésre kiválasztott kérdéseket kifejezetten azért jelöltem ki, hogy tükrözzék a résztvevők technológiai aspektusokkal kapcsolatos ismereteit, valamint az adatokkal kapcsolatos aggodalmaikat. Ezek a kérdések többek között a következőket tartalmazták: „Az autója képes csatlakozni az internethez?”, „Az Ön autója „okosautó” volt vagy az jelenleg?”, „Úgy gondolja, hogy az autója adatokat küld (küldött) a gyártónak?”, „Úgy gondolja, hogy az autója adatokat küld (küldött) harmadik feleknek?”, és „Úgy gondolja, hogy családtagjai autói adatokat küldenek a gyártónak vagy más vállalatoknak?”

Ezek a kérdések tematikailag kapcsolódnak az okosautó-technológiához és az adatbiztonséghoz, melyekről feltételezhető, hogy a válaszadók általános tudatosságának és észlelésének összefüggő dimenzióit reprezentálják. A kérdésekre adott válaszok konzisztenciájának értékeléséhez a Guttman-féle Lambda 2-t[77] (gyakran Lambda-2-ként jelölve), egy megbízhatósági együtthatót alkalmaztan, amely rugalmasabb megközelítést kínál a Cronbach-alfa mellett, mely elterjedt ugyan, viszont korlátozó feltételezéseken alapul.[78] A Cronbach-alfa például azt feltételezi, hogy minden tétel ugyanazt a konstrukciót méri, és folyamatos vagy Likert-skálán elhelyezhető adatokat igényel.[79] Adataim azonban dichotóm válaszokat (Igen/Nem) tartalmaztak, valamint „Nem biztos” opciót, amelyet 0,5-es középértékként kódoltunk.

Elméleti síkon a Guttman-féle Lambda a klasszikus tesztelméleten alapul, amely a válaszok tételek közötti konzisztenciájának vizsgálatával kívánja becsülni a

megbízhatóságot. A Lambda 2 kifejezetten olyan alternatív megbízhatósági mérőszámként lett kialakítva, amely figyelembe veszi az egyes tételek varianciáit és a tételek közötti kovarianciákat. A Lambda 2 a megbízhatóságot az egyes tételek varianciájának és a tételek közötti kovarianciáknak (kapcsolatoknak) vizsgálatával számítja ki. A Lambda-2 lényegében a válaszok (tételek) közötti konzisztenciát és azt méri, hogy ezek mennyiben járulnak hozzá egy adott összpontszámhoz. Matematikailag az összesített tételpontszámok teljes varianciáján, valamint az egyes tételek varianciáin és kovarianciáin alapul.

A Guttman-féle Lambda 2 megközelítése iskolai tesztek vizsgálatán alapul és abból a gondolatból indul ki, hogy ideális esetben minden tesztnek képesnek kell lennie arra, hogy megkülönböztesse a tesztalanyok képességeit (ellenkező esetben a tesztelésnek nem lenne értelme). Ez a szemléletmód alkalmazható a kérdőíves kutatások esetén is.

A kapott λ-2 érték eredményeinek kategorizálása:

- ≥0,70 alkalmas csoportszintű vizsgálatokhoz, értékelésekhez.
- ≥0,80 alkalmas alacsony tétű értékelésekhez, például oktatási visszajelzésekhez vagy kurzusértékelésekhez.
- ≥0,90 alkalmas magas tétű döntésekhez, mint például iskolai felvételi, pótlólagos elhelyezés vagy előléptetések.

Vizsgálatomban a Lambda-2 előnyös volt, mivel képes kezelni bináris és középértékre skálázott tételeket is, és nem követeli meg, hogy minden tétel egyenlő mértékben járuljon hozzá a mögöttes konstrukcióhoz.

A Guttman-féle Lambda-2 érték kiszámítási folyamata több lépésből állt a pontosság biztosítása érdekében. A kiszámításhoz python scriptet alkalmaztam, Jupyter Notebook környezetben. Első lépésként minden választ numerikus skálára konvertáltam: az „Igen” válaszokat 1-es, a „Nem” válaszokat 0-s, míg a „Nem biztos” válaszokat 0,5-ös értékkel kódoltuk. Az olyan irreleváns válaszokat, mint például „Soha nem volt autóm,” kizártam, mivel ezek nem járultak hozzá értelmezhető módon a mért konstrukcióhoz. Az adatok előkészítése után minden kérdésre vonatkozóan kiszámítottam az elemvarianciákat, valamint az összesített pontszámok összvarianciáját az összes elem esetében. A Lambda-2 kiszámítása során az egyes elemek varianciáinak összegéhez hozzáadtam a tételek közötti kovarianciák kétszeresét, amely megragadja, hogy egy kérdésre adott válaszok

miként jelezhetik előre a többi kérdésre adott válaszokat. Végül az így kapott együttes varianciát elosztottam a tételek összesített pontszámainak teljes varianciájával, amely eredményül adta a Lambda-2 együtthatót.

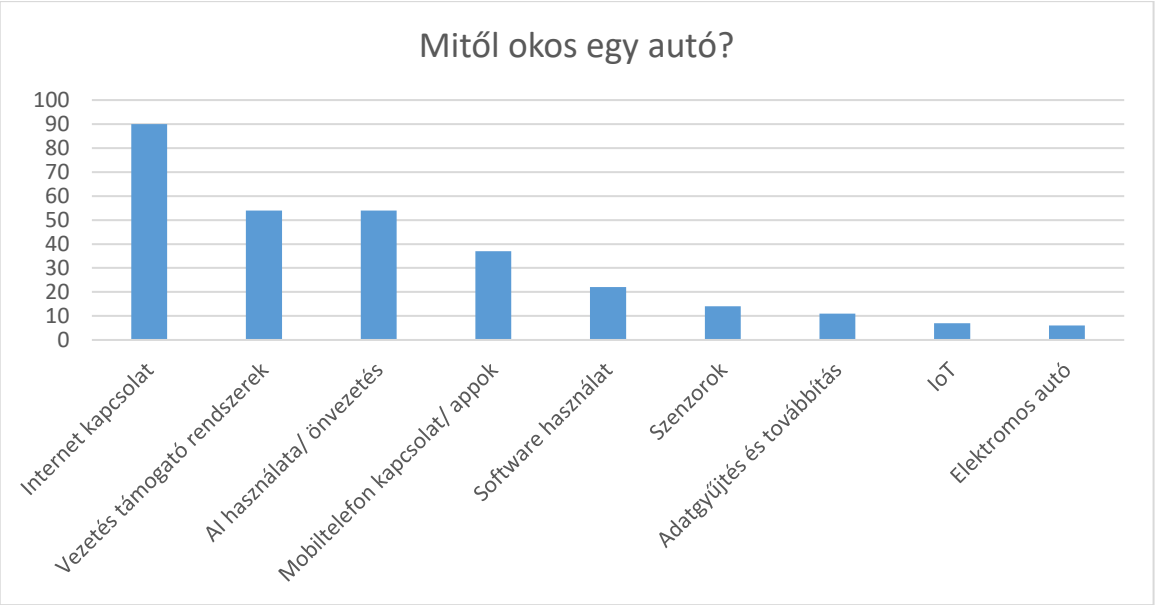
A körülbelül 1,0 értékű Guttman-féle Lambda-2 eredményünk tökéletes belső konzisztenciára utal, jelezve, hogy a kiválasztott kérdések szorosan összefüggenek és megbízhatóan mérnek egy közös gondolati konstrukciót az okosautó-funkciókkal és az adatvédelemmel kapcsolatos tudatosság és észlelés terén. Az ilyen magas Lambda-2 érték azt sugallja, hogy a válaszadók következetesen hasonló szintű tudatosságot vagy megértést mutattak a különböző kérdésekben, ami jól körülhatárolt, összetartó koncepciót tükröz. Ezáltal kizárható az az eshetőség, hogy valaki odafigyelés nélkül, véletlenszerűen válaszolta volna meg a kérdéseket.

A kapott eredmény megerősíti a kérdőíves adatok megbízhatóságát, igazolva, hogy a kérdések hatékonyak a résztvevők okosautóval kapcsolatos adatgyakorlatok iránti attitűdjeinek és tudásának együttes mérésében.

4.1.4 A válaszok elemzése és értelmezése

A kérdőíves kutatás során elsőként a válaszadók „okosautókkal” kapcsolatos definícióira voltam kíváncsi, azaz arra, mit értenek okosautó alatt, mitől „okos” egy autó. Miután napjainkban az okoseszközök részei az életünknek és az „okos” kifejezés népszerű hívószónak számít, a hétköznapi nyelvben ez a fogalom nehezen definiálható. A definíció mellett a szabadszöveges válaszadási lehetőség azt is biztosította, hogy további kapcsolódó koncepciókat is megfigyeljek – például azt, eszébe jut-e valamelyik válaszadónak a definíció megadása során az eszköz használatának kockázata (pl. hogy az autó vezeti önmagát az autópályán vagy rendelkezik a kapcsolt zenelejátszó alkalmazás preferenciaadataiaval, ami alapján következtetni tud a felhasználó hangulatára)?

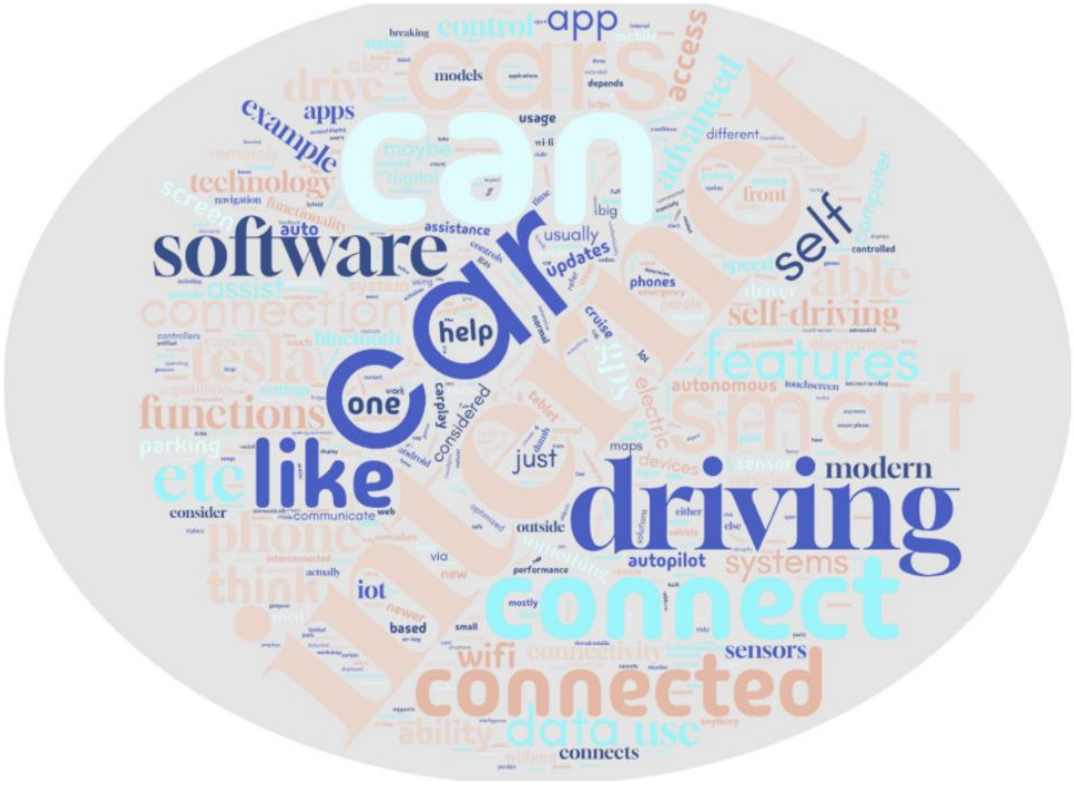
A válaszadók szöveges válaszai alapján megkerestem azokat a kulcsszavakat amelyek jellegzetesen előfordulnak a válaszokban amellyel az okosautó fogalmát definiálják.



4. ábra - A válaszadók definíciójában leggyakrabban előforduló gondolati koncepciók

A válaszok alapján jól látható, hogy az első fogalom ami a felhasználók eszébe jut az internetkapcsolat, de hogy milyen vonatkozásban, az változó. Legtöbben a vezetéstámogató rendszerekre, önvezető funkciókra asszociálnak, kevesen említik meg az adatgyűjtést és továbbítást. Ez kényelmi-funkció alapú megközelítést feltételez, tehát hogy a felhasználók az élményt biztosító funkcióra fókuszálnak a mögöttes működés mélyebb vizsgálata helyett.

A leggyakrabban előforduló fogalmakból szófelhőt készítettem, melynek bár tudományos relevanciája alacsony a pontos eredményekhez képest, azonban jól érzékelteti, mennyire ködös és tág az okosautó definíciója, illetve azt a megfigyelést is, hogy a felhasználó fókusza nem az adatküldés lehetőségén van.



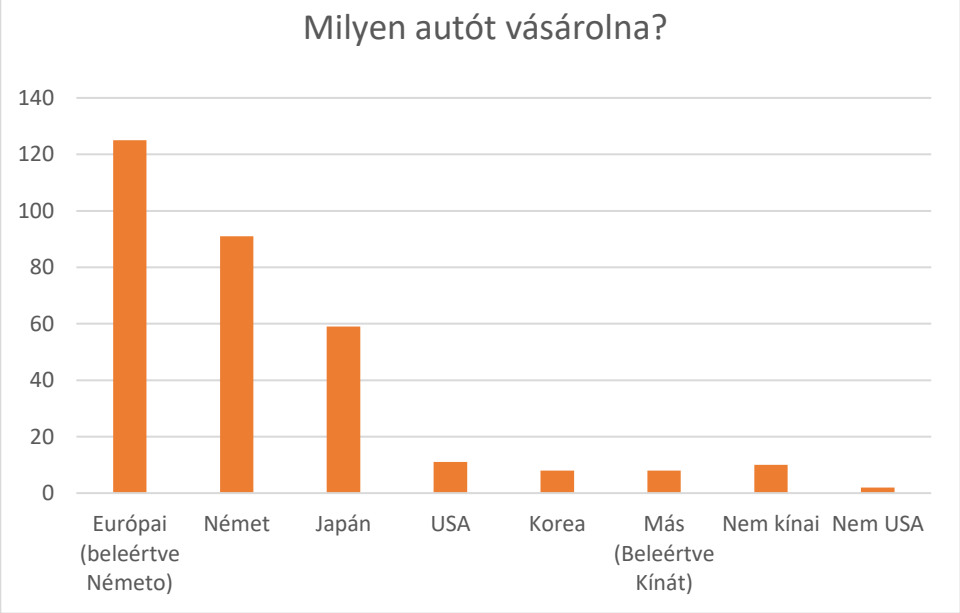
A következő kérdésben azt vizsgáltam hogy a válaszadóknak van-e preferenciájuk valamely származási országgal kapcsolatban. Származási ország preferencia során az első fontos adat, hogy egyáltalán hányan tartják fontos szempontnak a származási országot személygépjármű választásakor. Azok a válaszadók akik nem jelöltek meg származási ország preferenciát feltehetőleg nem tartják fontos szempontnak a származási országot, választásukat kizárólag más szempontok alapján teszik meg. Más válaszadók konkrétan megfogalmazták válaszukban, hogy kizárólag a felszereltség, fejlettség és egyéb teljesítményadatok alapján választanak illetve néhány válaszadó egyértelműen jelezte, hogy az ár a döntő nála és nem a származási ország. Ugyanakkor olyan válaszadó is volt akinél egyértelműen a fő szempont volt a származási ország negatív értelemben. A válaszadók között csak 10 francia származású személy szerepelt, de köztük jelentkezett a francia „patriotizmus”, a hazai termékek előtérbe helyezése, amelyeket a francia eladási adatok is tükröznek.[7] Egyik francia válaszadóm konkrétan úgy fogalmazott, hogy azért a francia járműveket preferálja, mivel ő maga is francia.

[7] https://cleantechnica.com/2024/11/02/evs-at-23-5-share-in-france-plugins-dip-as-hevs-surge/

5. ábra - A válaszadók személygépjárművválasztása és a származási ország relevanciája

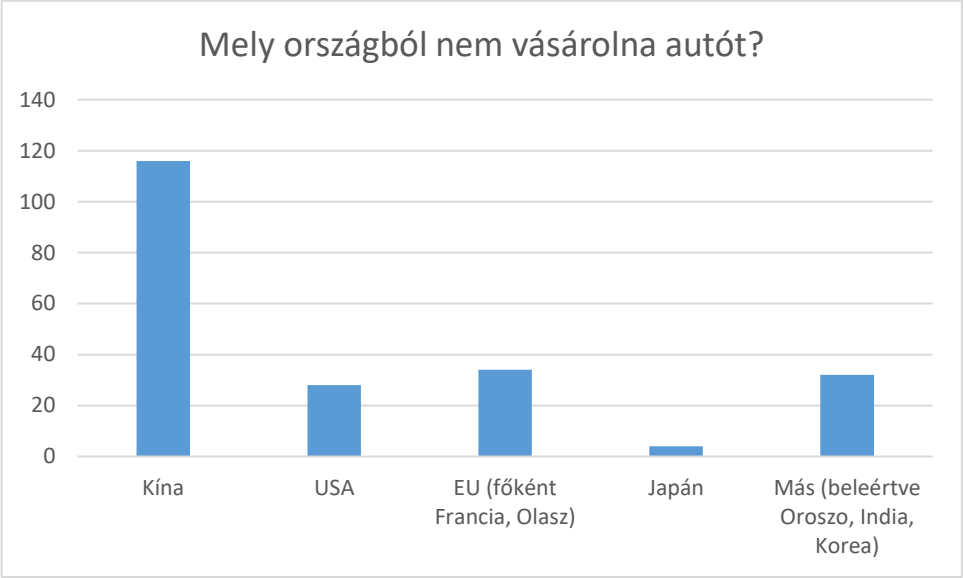
Látható, hogy a válaszadók közel kétharmada rendelkezik preferenciával valamilyen származási országra vonatkozóan, de ennek oka gyakran nem a biztonsági kockázatokkal függ össze. Az okokat később elemzem.

Az alábbi ábra az országpreferenciákat mutatja be a preferált származási országok bontásában. Ugyan a kérdés kifejezetten arra irányult hogy melyik országot preferálják, többen fontosnak tartották már itt megemlíteni hogy mely országot nem preferálják, pl: „mindegy, csak ne kínai legyen” a jármű. Bár ezek tagadó válaszok egy állító kérdésre, ezeket a válaszokat is szemléltettem az oszlopdiagramban, hiszen értékes információval bírnak.



6. ábra - Országpreferenciák származási országok bontásában

A kérdőívben rákérdeztem arra is, mely országok azok, amit a válaszadó kifejezetten kerül személygépjármű választásakor. A legtöbb válasz vélhetően vagy kimutathatóan geopolitikai hátterű döntéseken alapult (pl. Kína, Oroszország, mert ellenséges országok), némely válasz technikai képességeken (negatív értelemben, nem megbízható, esetleg túl fejlett) alapult (Kína és USA) más válaszok személyes tapasztalatokon alapultak (pl. „mindegy csak ne olasz legyen, azokkal csak bajom volt eddig").



7. ábra - Személygépjárművválasztáskor elkerült származási országok

A fenti oszlopdiagram jól tükrözi hogy a válaszadók nagy arányban (közel 40%) kerülik a Kínából származó személygépjárműveket. Az ok a válaszok alapján nem kizárólag geopolitikai jellegű és nem is feltétlenül az adatbiztonsággal vagy a kockázatokkal függ össze. A kínai autók kevésbé ismertek, az „olcsó de rossz kínai termék" emlékek sokakban még aktívan élnek.

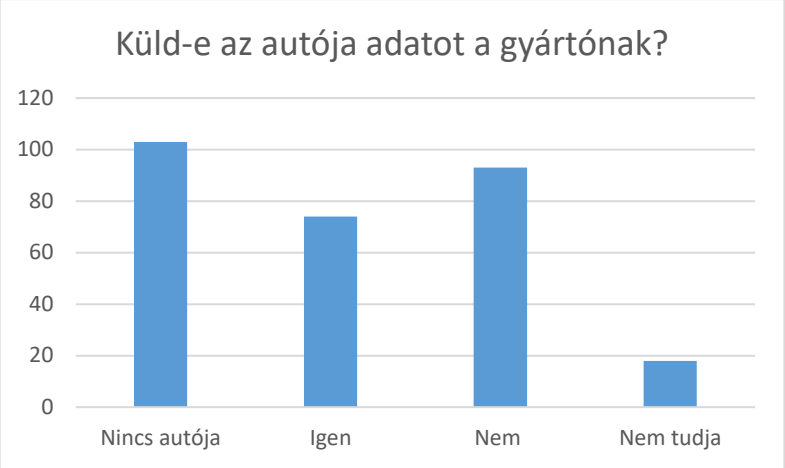
A következő ábrán az elutasítás okait elemeztem. A válaszadók indoklásaiból az is kiderül, hogy milyen ok vagy okok miatt nem preferálják a megnevezett országokat.

8. ábra - A nem preferált származási országokkal kapcsolatos ellenérzések természete kategóriákra bontva

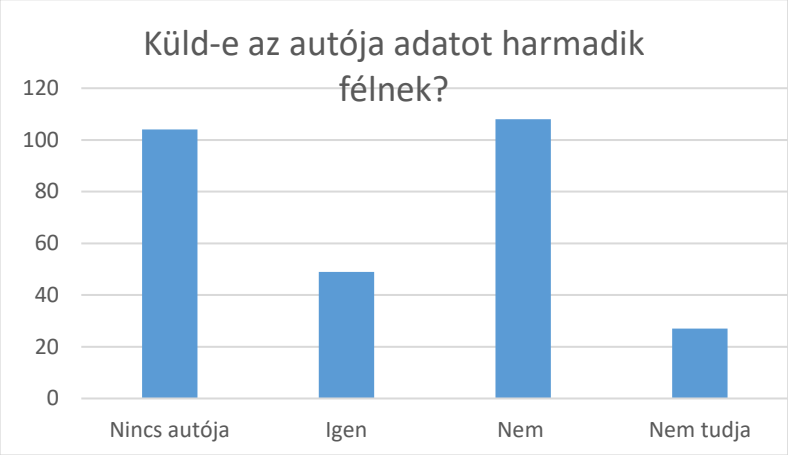
Néhány válasz esetében nehéz eldönteni, hogy geopolitikai vagy biztonsági aggályok állnak-e a háttérben – vagy mindkettő, – mivel a két kategória összefügg. Az alábbi választ „China, because of privacy reason" (azaz „Kína, adatvédelmi okokból") - a biztonsági kategóriába helyeztem, de más válaszokat pl: „China they use surveillence everywhere" (azaz „Kína, megfigyelést alkalmaznak mindenhol") geopolitikai okként jelenítettem meg. Mindezek ellenére a határok a geopolitikai és a biztonság között számos esetben elmosódnak. Az oszlopdiagram jól mutatja, hogy a legjelentősebb ok geopolitikai, többen meg is nevezték hogy attól tartanak hogy személyes adataik egy másik országba, ezáltal rossz kezekbe kerülnek.

Az elemzés során a kvalitatív válaszok halmazokba csoportosításával tehát képet kaptunk arról, hogy a válaszadók általában negatívan viszonyulnak az adatok továbbításához, különösen, ha azt egy saját országon kívüli vállalathoz, egy-két konkrét országba, illetve a felhasználó tudta nélkül végzik (lásd később).

Az eddig elemzett válaszok alapján az általános hozzáállást, általános aggályokat próbáltam feltérképezni. A kérdőív további részében konkrétan is rákérdeztem, tartanak-e a válaszadók attól hogy járművük adatokat továbbíthat valahová. Az első két kérdésben a válaszadóknak arra kellett válaszolniuk hogy tudnak-e arról, hogy az autójuk adatokat küldhet a gyárnak vagy harmadik félnek (például adatelemző cégeknek).

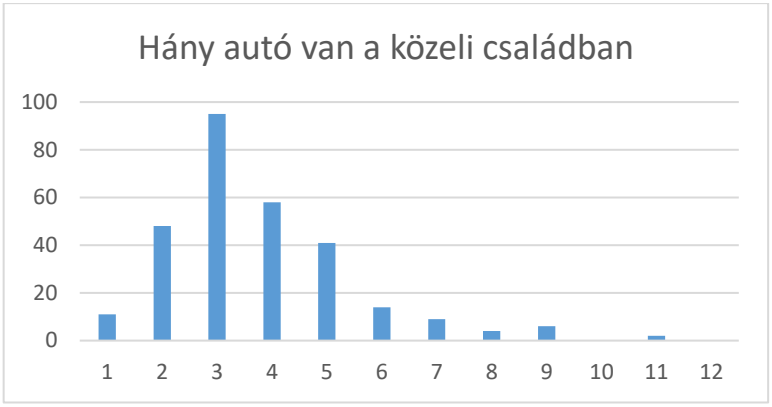


9. ábra - Kérdőíves kérdés a személygépjármű által küldött adatokra vonatkozóan (gyártó)

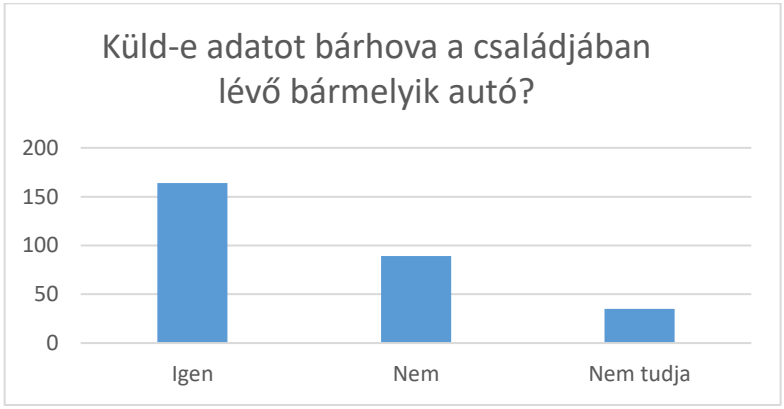


10. ábra - Kérdőíves kérdés a személygépjármű által küldött adatokra vonatkozóan (harmadik fél)

A következő kérdésben rákérdeztem arra is hogy mit gondol a családjában lévő személygépjárművek adatküldési szokásairól. A legtöbb esetben a közeli családban 2-5 autó van a válaszok alapján, így ezek a gondolatok abban az esetben is érdekesek lehetnek, ha egy válaszadónak nincsen saját személygépjárműve. Ezzel nagyobb minta vizsgálható, azonban mégis jól elkülönül a közvetlen saját tapasztalat a közvetett tapasztalattól.



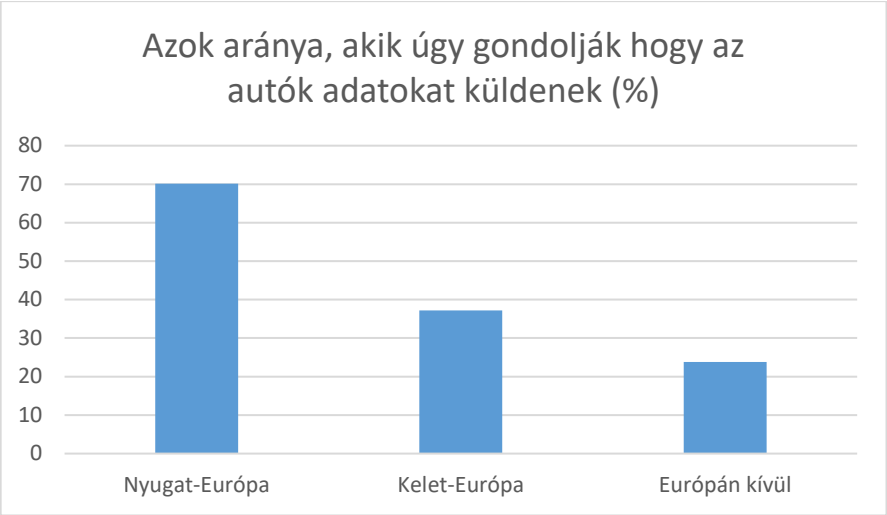
11. ábra - A kérdőív válaszadóinak családjának tulajdonában lévő személyautók száma



12. ábra - A család tulajdonában lévő személyautók adatküldésére vonatkozó gondolatok

Érdekes összevetni a saját autóra és a családban lévő autókra vonatkozó kérdésekre adott válaszokat. A családban lévő autókra irányuló kérdésekre a válaszok lényegesen negatívabbak. Mindez azt jelentheti, hogy ha konkrétan megnevezzük a kockázatot (a kérdésfeltevéssel magával felhívtam a kérdőívalanyok figyelmét arra, hogy járművük adatot küldhet – miközben lehetséges, hogy ez eszükbe sem jutott korábban) akkor a válaszadók fókusza jobban ráterelődik a veszélyre (a szerettei adatainak esetleges kiszivárgására, visszaélésekre).

Az adatküldéshez való viszonyulás az egyes válaszadói származási országok esetében eltérőek, így az adatküldéssel kapcsolatos kérdések esetében a válaszadó nemzetisége alapján is elemeztem a válaszokat.

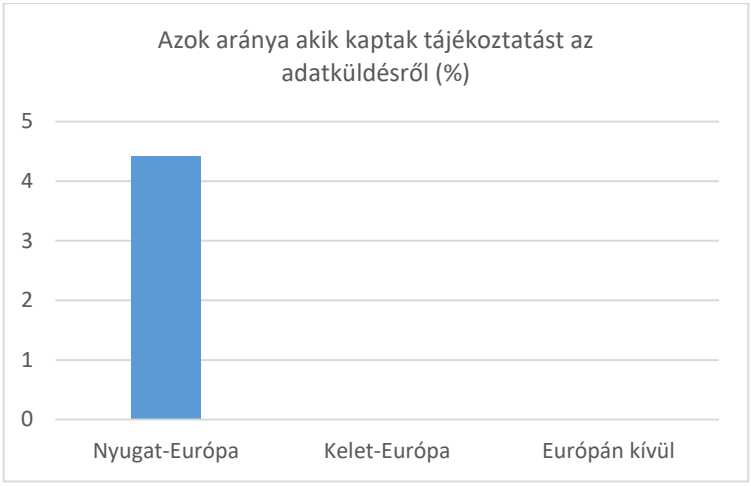


13. ábra - Azok aránya, akik úgy gondolják, hogy a személygépjárművek továbbítanak adatokat - származás szerinti bontásban.

A kérdőív része volt két további eldöntendő kérdés, amelyek az adattovábbításra vonatkoztak. Az első kérdés arról szólt, hogy kapott-e valaha valamilyen tájékoztatást a válaszadó, hogy az autója adatokat küldhet . A válaszokat egyben és nemzetiségek alapján is elemeztem.

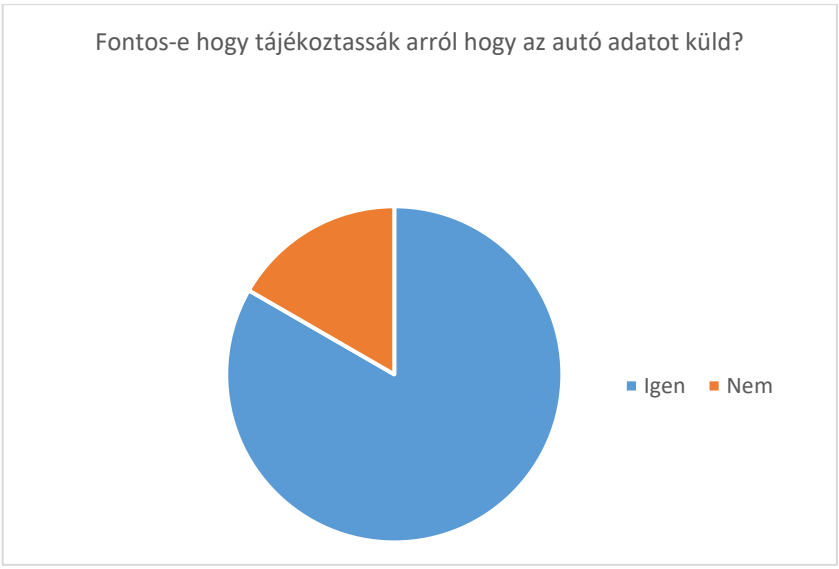
14. ábra - Válaszok arra a kérdésre vonatkozóan, hogy a személygépjárműtulajdonosok kaptak-e valaha tájékoztatást a jármű adattovábbítási folyamataira vonatkozóan.

Fontos megjegyezni, hogy az „Igen” válaszok között szerepelt olyan válaszadó is, aki a szerviz által fizikailag lekért adatokra gondolt annak ellenére, hogy a kérdés nem erre vonatkozott. Ezekben az esetekben a tájékoztatás is mást jelent, hiszen ilyenkor a szerviz a saját maga által elvégzett feladat kapcsán is tájékoztatja a felhasználót, amibe beletartozik, hogy esetleg lekérte a diagnosztikai adatokat valamilyen eszközzel, például OBD porton keresztül.



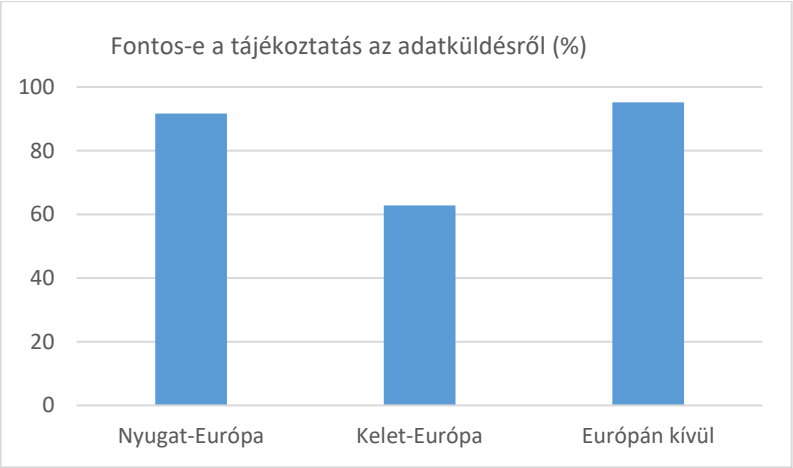
15. ábra - Azok aránya, akik kaptak tájékoztatást az adattovábbításról területek szerinti bontásban.

A második eldöntendő kérdés arra vonatkozott, hogy a válaszadó fontosnak tartja-e hogy tájékoztassák amennyiben az autója adatokat küld a gyártó vagy más szereplő felé.



16. ábra - Az adattovábbítással kapcsolatos tájékoztatás fontossága a válaszadók szerint

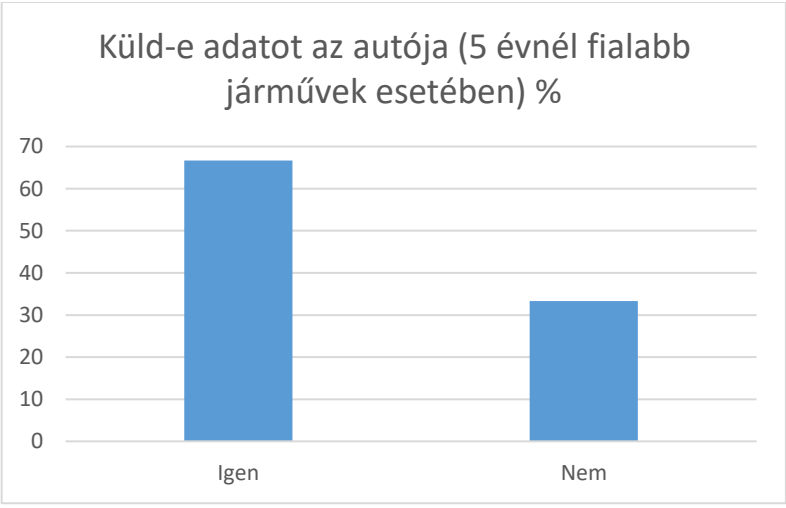
Az eredményekből látható, hogy a válaszadók nagy része fontosnak tartja, hogy ha az adattovábbítás megtörténik, akkor tájékoztatást kapjanak erről. Érdekes megfigyelni, hogy vannak olyan válaszadók is, akik ezt az információt nem tartják fontosnak, a kérdőív megalkotása során azonban ezt nem vettük figyelembe, így ennek okára sem tértünk ki. Egy jövőbeli kutatás során azonban érdemes lehet ezt a kérdést is vizsgálni.



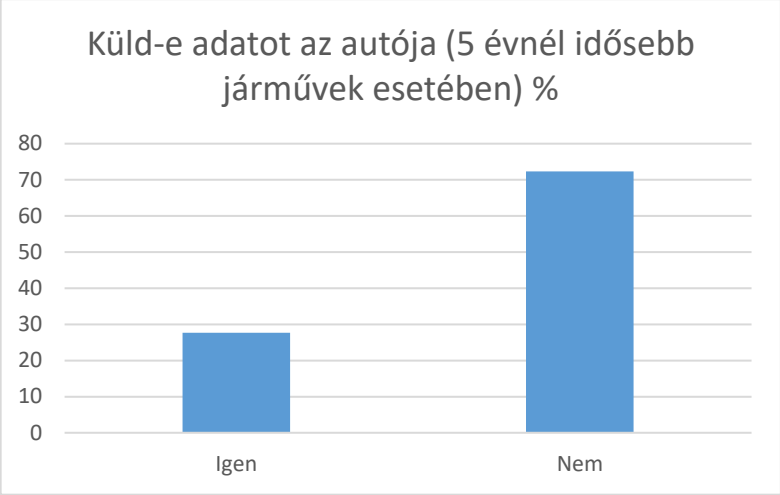
17. ábra - Az adattovábbítással kapcsolatos tájékoztatás fontossága a válaszadók szerint területi bontásban

A területi megoszlást vizsgálva az derül ki, hogy nincsen jelentős küldönbség – azaz az adattovábbítással kapcsolatos tájékoztatás fontossága ugyanúgy felmerül a különböző politikai rendszerek alapján működő országokban élő válaszadók esetében (bár mivel ennek a kérdésnek a részletes vizsgálata nem képezte az értekezés scope-ját, illetve némelyik országokból csak csekély számú válaszadó válaszolt, így csak az aggregált adatok kerültek vizsgálatra és az egyes konkrét országokra vonatkozóan nem tehető ilyen megállapítás).

Ha a személygépjárművek korával összefüggésen vizsgáljuk az adattovábbítás kérdéskörét, akkor a következő eredményre juthatunk:



18. ábra - Az adattovábbítással kapcsolatos tudatosság 5 évnél fiatalabb járművek esetén



19. ábra - Az adattovábbítással kapcsolatos tudatosság 5 évnél idősebb járművek esetén

Bár a pontos személygépjárműtípust nem ismerjük (a kérdések között szerepelt a típusra vonatkozó kérdés, azonban a válaszok nem bizonyultak elég pontosnak), az 5 évnél fiatalabb járművek esetében jellemző az adattovábbítás valamely irányba, így szembetűnő a „Nem” válaszok magas aránya.

4.2 Eredmények összegzése

A válaszadók adatküldési tudatosságára vonatkozóan megállapítható, hogy 35,8% egyáltalán nem birtokolt járművet, 32,3% pedig úgy véli, hogy járműve nem küld adatokat a gyártónak vagy harmadik feleknek. Ugyanakkor 25,7% úgy gondolja, hogy járműve adatokat küld a gyártónak, míg 6,3% bizonytalan ebben.

Az adatkezelési tájékoztatás szintjét illetően a válaszadók túlnyomó többsége (82,8%) nem kapott tájékoztatást a jármű által továbbított adatokról, és mindössze 14% nyilatkozott úgy, hogy kapott valamilyen formában információt (például adatvédelmi tájékoztató vagy szervizelés során). Azok, akik kaptak információt, gyakran említették, hogy e-maileken keresztül tájékoztatták őket, míg néhány válaszadó megemlítette, hogy a szerviz vagy a márkakereskedés részéről érkezett a tájékoztatás.

A kérdőíves válaszok elemzése után az alábbi megállapításokat tettem:

- Az „okosautó” fogalma meglehetősen heterogén gondolatokkal övezett a válaszadók körében. Sokan az internetkapcsolat miatt tartják a személygépjárművet okosnak, mások a fejlett szoftverkörnyezet és az MI technológia miatt, van olyan válaszadó is, aki a kényelmi funkciók miatt gondolja

autóját okosnak. A jármű azon tulajdonsága, hogy képes adatokat küldeni folyamatosan és adatokat fogadni nem ismeretlen a válaszadók számára, de kevesen tartják ezt kiemelt szempontnak a meghatározás során (azaz vélhetően magától kevés személy gondol bele ebbe az aspektusba).

- A személygépjárművek származási ország szerinti elutasítottsága a Kínai Népköztársaság esetében nagyon erős a nyugat-európai válaszadók esetében. Az elutasításuk fő oka geoploitikai jellegű, a minőségi aggályok – bár hangsúlyosak – csak másodlagosak az elutasítás kapcsán.
- Amennyiben konkrétan megnevezzük a problámát: „a jármű adatokat továbbíthat", a válaszadók nagy része elfogadja és felismeri a kockázatokat, de ha saját járművükről van szó, akkor kevésbé élik meg negatívan ezt a tényt, mint általánosságban (családban található személygépjárművek adattovábbítási képessége).
- Számos válaszadó nincsen tisztában azzal, hogy a járműve adatokat továbbít, arról pedig még kevesebben tudnak, hogy ezek az adatok akár harmadik félhez is eljuthatnak. Ezzel összefüggésban viszont többségük tart az adatgyűjtés kockázataitól.

Ez az elemzés alátámasztja a H3 hipotézist, miszerint a személygépjármű-tulajdonosok nem rendelkeznek elegendő tájékoztatással a járműveik által végzett adattovábbításról. Az eredmények azt sugallják, hogy az információbiztonsági tájékoztatás mértéke jelentősen elmarad a szükségestől, ami arra utal, hogy a tulajdonosok többsége nincs tisztában azzal, milyen adatokat oszt meg a járműve a gyártóval vagy más harmadik felekkel, valamint hogy milyen kockázatokat hordoz magában a járművek adatkezelése.

5. MÉLYINTERJÚK – HAZAI SZAKÉRTŐK TAPASZTALATA

Ebben a fejezetben az IoT (Internet of Things) koncepciójának alkalmazhatóságát vizsgálom a személygépjárművekre mint hálózatba kötött eszközökre, az információbiztonság szempontjából. A fejezet célja a H4 hipotézis alátámasztása, amely szerint a személygépjárművek biztonságos informatikai eszközként való kezeléséhez elengedhetetlen egy átlátható adattovábbítási rendszer, titkosított adatforgalom és egy felügyeleti hatóság kijelölése. A jelen fejezet az IoT szabványok és definíciók rövid elemzésével kíván rávilágítani arra, hogy a személygépjárművek számos szempontból

párhuzamba állíthatók az IoT eszközökkel, és így ezen szabályozások alkalmazása hozzájárulhat a járművek adatbiztonságának erősítéséhez. A fejezet a szakirodalmi háttér, valamint a személygépjárműveket IoT eszközként kezelő megközelítések gyakorlati kihívásait elemzi, és arra fókuszál, hogy az adattovábbítás szabályozásának milyen jelentősége lehet az autóipar biztonsági szabványainak átfogó fejlesztésében.

Másrészt jelen fejezet a személygépjárművek információbiztonsági kockázatainak gyakorlati kezelési módjait is vizsgálja, és célja a H5 hipotézis alátámasztása is, amely szerint egy átfogó kockázatmenedzsment keretrendszer, amely figyelembe veszi az adatkezelés, adattárolás és adattovábbítás valamennyi aspektusát, hatékonyan hozzájárulhat a járművek biztonságának növeléséhez. A fejezet a kvalitatív interjúk alapján összegyűjtött szakértői vélemények elemzésére épít, amelyek gyakorlati példákkal mutatják be az autóipar kiberbiztonsági szabályozásának hiányosságait és kihívásait. A vizsgálat fókuszában az a kérdés áll, hogy milyen tényezők befolyásolják a szabályozások betartását és hatékonyságát, valamint hogyan lehetne egy átfogóbb kockázatkezelési szemlélettel elősegíteni a személygépjárművek információbiztonságát.

Bármilyen szervezet biztonsági szintjének mérése információbiztonsági szempontból erősen szubjektív tényezőkön alapul, már csak azért is, mert ahogyan az már a korábbi fejezetekben is szerepelt, a szabványok és jogszabályok jellemzően nem hivatottak a „hogyan”, azaz a mérési módszertanra vonatkozó kérdések megválaszolására. A cél az, hogy minden szervezet maga alakítson ki egy számára megfelelő logikusan felépített és átlátható struktúrát, amely – valamilyen saját maga által jónak tartott módszertannal – képes megmutatni a biztonság szintjének növekedését egy adott bázisévhez képest (jellemzően auditciklusonként).

Az információbiztonsági kihívásokra, illetve megoldási lehetőségre vonatkozóan ebből az okból kifolyólag nem lehet következtetni egyszerű kérdőíves adatgyűjtések és elemzések alapján.

Másrészt a téma jellegénél fogva bizalmi alapú megközelítést igényel és ezért bármilyen kvalitatív megközelítés erősen korlátozza úgy a válaszadók körét, mint a feltehető kérdések mélységét és számát, hiszen a leírt információk alapján statisztikai alapon beazonosíthatók maradhatnak az interjúalanyok vagy szervezetek – akár az adatok anonimizálását követően is. [80] Ennek következtében kizárom a nagy mintán elvégzett statisztikai módszerek alkalmazását.

Az internetkapcsolatra képes személygépjárművek hasonlóan a mobiltelefonokhoz, ki vannak téve az internetről érkező támadásoknak, miközben a személygépjármű rendszereihez való illetéktelen hozzáférés használatának célját tekintve nagyobb veszélyforrást jelenthet annak felhasználójára, mint egy mobiltelefon. A modern személygépjárművek a „Dolgok Internetéhez" (Internet of Things, IoT) hasonlóan képesek arra, hogy az internethez kapcsolódjanak és onnan különböző utasításokat tartalmazó üzeneteket fogadjanak. Egyre több gyártó tér át a gépjárművek belső hálózatának kulcsfontosságú elemei, a mikrokontrollerek (ECU – *electronic controller unit*) *firmware*[8] progjamainak (alapszoftver vagy vezérlőprogram) interneten keresztül való frissítésére is. Ezt a gyakorlatot FOTA/OTA szolgáltatásnak (*over-the-air* vagy *firmaware* esetében *firmware-over-the-air*[9]) nevezzük.

A személygépjárművek ma már a legkülönfélébb szenzorokkal, adatfeldolgozó egységekkel, rögzítőeszközökkel (pl. kamera) vannak felszerelve, melyek nagy mennyiségű információ összegyűjtésére szolgálhatnak. Az ilyen adatokból a felhasználó vagy egy csoport számos tulajdonságára, szokására lehet következtetni, mely szintén biztonsági kockázatokat rejt magában. Ugyan a gépjárműiparban a mind a gyártóknak, mind pedig a beszállítóknak szigorú biztonsági előírásoknak kell megfelelnie, az informatika gyors fejlődésének hatására ugyanezt a szigorú rendszert az elektronikus információbiztonság kapcsán már sokkal nehezebb működtetni. [81] Bár a legtöbb esetben a támadóknak nem érdekük a járműben tartózkodók életét veszélyeztetni, mégis van ok az aggodalomra, hiszen a rengeteg gyűjtött adatnak köszönhetően magas haszonnal kecsegtethet egy esetleges sikeres behatolás. [82] A megfelelő védelem kialakítása kapcsán problémát jelent, hogy a biztonsági értékelés gyakran szubjektív szempontok alapján történik – minél összetettebb rendszerről van szó, annál nehezebb pontos metrikát alkalmazni a kockázatok elemzésére. [83], [84]

Az információbiztonsági szakértők szubjektív ítéletei fontos szerepet játszanak a kiberfizikai rendszerek fenyegetéseinek értékelése és modellezése során. Például az egyes rendszerelemek sebezhetőségét többféle tényező alapján lehet leírni; ilyenek a bonyolultság, a technológiai érettség és a támadások segítésére rendelkezésre álló

[8] Hardverben - jellemzően csak olvasható memóriában (ROM) vagy programozható csak olvasható memóriában (PROM) - tárolt számítógépes programok és adatok, úgy, hogy a programok és adatok nem írhatók vagy módosíthatók dinamikusan a programok végrehajtása során.

[9] A folyamat során a szoftverfrissítés „a levegőn keresztül", azaz internet kapcsolat segítségével jut el a járműhöz, tehát nincs szükség például pendrive vagy egyéb fizikai eszköz csatlakoztatására.

eszközök elérhetősége. Ezek az információk hasznosak a támadási kockázat meghatározásában, de nagy részüket nehéz automatikusan begyűjteni. Azonban a legtöbb szakértőben valamilyen mértékű bizonytalanság rejlik az értékelések terén. [85] A meglévő módszerek a fenti okokból kifolyólag nagymértékben függnek az értékelő tapasztalataitól, és a biztonsági mérőszámok általában legjobb esetben belső kockázatelemzési metódusok eredményeiként alakulnak ki. [86]

Jelen fejezet célja, hogy feltárja a személygépjárművekkel kapcsolatos információbiztonsági kihívásokat és javaslatokat fogalmazzon meg a jelenleg használatban lévő szabványok és szabályozási környezet gyakorlati alkalmazásával kapcsolatban. A vizsgálat célja továbbá az is, hogy javaslatokat fogalmazzon meg a szabályozási környezet tartalmára és alkalmazására vonatkozóan a személygépjárműipar területén, továbbá egy a kiberbiztonsági területen kevésbé gyakran alkalmazott módszertani megközelítéssel vizsgálja meg a témát, ezzel hozzájárulva a jövőbeli kutatási irányok meghatározásához.

5.1 Mélyinterjúk

A Dolgok Internete, azaz az "Internet of Things" (IoT) kifejezést Kevin Ashton alkotta meg 1999-ben, egy előadáson a Procter & Gamble-nél. [87] Az IoT eszközök fogalmára azóta többféle definíció is elterjedt, melyek közül néhány gyakran alkalmazottat az alábbi táblázatban szemléltetünk:

Forrás	Definíció
NIST SP 1800-16B-C	Eszközök hálózata, amely tartalmazza a hardvert, szoftvert, firmware-t és aktuátorokat, amelyek lehetővé teszik az eszközök kapcsolódását, kölcsönhatását és szabad adat- és információcsere lehetőségét.[10]
NIST SP 800-172	A kiadványban használt értelemben olyan felhasználói vagy ipari eszközök, amelyek csatlakoznak az internethez. Az IoT eszközök szenzorokat, vezérlőket és háztartási készülékeket is magukba foglalnak.[11]
Gartner	Az "Internet of Things" (IoT) a fizikai tárgyak hálózata, amelyek beépített technológiával rendelkeznek, hogy

[10] https://csrc.nist.gov/glossary/term/internet_of_things
[11] https://csrc.nist.gov/glossary/term/internet_of_things

	kommunikáljanak, érzékeljenek vagy kölcsönhatásba lépjenek a belső állapotukkal vagy a külső környezettel.[12]
Európai Parlament	Az „Internet of Things” (IoT) olyan elosztott hálózatot jelent, amely fizikai tárgyakat köt össze, képesek érzékelni vagy cselekedni a környezetükben, és kommunikálni egymással, más gépekkel vagy számítógépekkel.[13]

10. táblázat - IoT definíciók (Saját szerkesztés)

A személygépjármű IoT eszközként való értelmezése az elemzett szakirodalmi anyagban nem szerepel ugyan, azonban ha arra gondolunk, hogy a napjainkban használt személygépjárművek szenzorokkal és internetkapcsolattal rendelkeznek, és a telekommunikációs hálózatokon keresztül a szenzorok által rögzített adatokat (vagy azok feldolgozásának eredményét) továbbítják a gyártó vagy harmadik felek szervei felé, akkor az 1. táblázatban felsorolt definícióknak megfelel.

Ez a megfigyelés azért tarthat számot érdeklődésre, mert az IoT eszközök sajátosságaikat tekintve sokkal közelebb állnak a jelenleg használt személygépjárművekhez, mint a 20-30 évekkel ezelőtti, külső hálózati kommunikációt egyáltalán nem használó régi személygépjárművekhez. Ennek okán a rájuk vonatkozó meglévő szabályozási környezet alkalmazása, illetve a jövőbeni szabványok szinergikus megalkotása megoldást jelenthetne a személygépjárművek biztonságának biztosítására. Az IoT eszközök standardizálása azonban mindmáig komoly kihívásokba ütközik, köszönhetően a technológia gyors fejlődésének, az eszközök rövid életciklusának és sokféleségének. [88] Ezek a kihívások szintén megfigyelhetőek a személygépjárművek esetén.

5.2 Módszertan

A kutatás módszertanaként a téma érzékeny mivoltát és összetettségét figyelembe véve a mélyinterjút választottam. A mélyinterjú sajátossága, hogy a kutató nem megadott kérdéslista, hanem előre definiált témakörök alapján folytat dialógust az interjúalanyokkal azzal a céllal, hogy lehetőséget kapjon olyan kontextuális információk megszerzésére is, melyek az előzetes kutatások alapján nem merültek fel. [89] A

[12] https://www.gartner.com/en/information-technology/glossary/internet-of-things
[13] https://www.europarl.europa.eu/RegData/etudes/BRIE/2015/557012/EPRS_BRI(2015)557012_EN.pdf

mélyinterjú nem alkalmas ugyan arra, hogy a kapott eredmények alapján általánosításokat fogalmazhassak meg, de lehetőséget biztosít arra, hogy a tématerületet mélyen ismerő szakemberek tapasztalatait és javaslatait megismerjük és összefoglaljam.

Jelen kutatás lefolytatásához ezért a terepkutatás kategóriájába tartozó féligstrukturált interjúztatás módszere került kiválasztásra, mint a témához illeszkedő technika. [90] Az empirikus kutatás célja egyrészt annak megismerése, hogy mi a magyar szakértők véleménye a szakirodalomban felvetett információbiztonsági szabályozásokkal kapcsolatos trendekről, érdemes-e IoT eszközként kezelni a személygépjárművet és milyen kihívásokkal szembesülnek az elméletek gyakorlati adaptálása során, másrészt pedig az, hogy a felmerült információbiztonsági problémákkal kapcsolatos megoldási javaslatok összegyűjtésre kerüljenek. Mivel ez a megközelítés mélyebb dialógust igényel és nem oldható meg például egyszerű kérdőíves módszertannal, ezért indokolt a mélyinterjúk alkalmazása. [91] Az interjú a kérdésfeltevésén és az arra adott válaszok megvitatásán kívül kötetlen formában zajlott, azaz interaktív beszélgetés keretében, ami megkönnyítette a többletinformációk megszerzését. [92] Az interjúk készítése közben fontos szempont volt olyan új információk feltárása, melyek a szakirodalmi elemzés során nem merültek fel, de újabb vizsgálatok alapját képezhetik.

A megfelelő kérdések megállapításához, először a fenti fejezetben körüljárt témákra alapozva négy dimenzió – személygépjármű mint IoT eszköz, információbiztonsági szabványok hatékonysága és alkalmazása, kihívások a szabványok és jogszabályok gyakorlati alkalmazásában, megoldási javaslatok – elkülönítése történt meg, amelyek sorbarendezésének szempontja az volt, hogy az általánosabb témakörtől tartsanak az egyre specifikusabb felé. Erre azért volt szükség, hogy meghatározható legyen, hogy a kiválasztott szakemberek milyen általános megközelítést alkalmaznak a munkájuk során és milyen specifikumokat fedeznek fel a személygépjárműipari információbiztonsággal kapcsolatban.

Mivel nem minden szakértő rendelkezik ugyanolyan mély tapasztalattal az autóipar kapcsán – de ettől függetlenül lehetnek releváns szakmai észrevételei, melyek az autóiparra is érvényesek (pl. mobileszközök vagy IoT eszközökre vonatkozó megoldások ismeretében) – így fontos, hogy az iparágspecifikus kérdések csak kiegészítő információk gyűjtésére szolgáltak és csak abban az esetben kérdeztem rájuk, ha az adott interjúalany ténylegesen rendelkezett ilyen jellegű tapasztalattal is.

5.2.1 Narratív elemzés

Ahhoz, hogy az információbiztonsági szabványok alkalmazásának nehézségeit gyakorlati szempontból vizsgálhassam, olyan technikával volt szükséges elemezni az interjúk lefolytatása során keletkezett információkat, amely segítségével nem csak egy-egy tény állapítható meg [93] az auditori munkával és a szabványokkal kapcsolatban, hanem azonosíthatók az elmélet és gyakorlat közötti különbségek mélyebben meghúzódó okai, vagy például az eredményeket befolyásoló szubjektív tényezők.

Az interjúleiratok a Krippendorff-féle tartalomelemzési módszertannal kerültek elemzésre, melynek lényege, hogy a kontextus is szerves részét képezi a szövegelemzésnek, így illeszkedik a tanulmányban foglalt komplex témához azáltal, hogy lehetőséget nyújt arra, hogy a kutató induktív módon következtessen a tartalomra. [93]

5.2.2 Mintavétel

A kvalitatív, mélyinterjús kutatás központi alanyai az információbiztonsági szakértők, azaz felkészítő és minősítő auditorok, tanácsadók és kutatók. Ahhoz azonban, hogy az elemzés során releváns információkat fedhessünk fel, szükség volt az előzetes, 25 főből álló csoport szűkítésére. A kutatásban résztvevő 10 interjúalany kiválasztása során szűrőfeltétel volt az információbiztonsági szakmák valamelyikében eltöltött minimum 5 év munkatapasztalat, illetve a minimum 5 különböző iparágban vagy területen szerzett jártasság. Ezek a kritériumok biztosítják, hogy a szakértők megfelelően széleskörű gyakorlati ismeretekkel rendelkezzenek a kutatott kérdéseket illetően. A személygépjárműiparban szerzett tapasztalat nem volt azonban követelmény, mivel jellegüknél fogva a kutatási kérdések megválaszolásához nem szükséges mély ágazati ismeret, ellenben a minél széleskörűbb rálátás a különböző iparágak szabályozási környezetéről hozzásegít a jó és rossz gyakorlatok felismeréséhez.

Ennek okán került a mintába például olyan szakember, aki főként magyar kis- és középvállalkozásokkal foglalkozik és olyan, aki jelenleg az állami szférában dolgozik, azonban korábbi ügyfelei és munkáltatói közé tartoznak pénzintézetek, gyógyszeripari gyárak és élelmiszeripari vállalatok is.

5.3 Eredmények

Az interjúalanyok válaszaiból kiderül, hogy három válaszadó dolgozott már valamilyen járműiparral kapcsolatos információbiztonsági projekten, feladatkörben, míg hét

személy nem rendelkezik ilyen tapasztalattal. Ennek okán csak az előbbi három személy számára tettünk fel iparágspecifikus, kifejezetten járműipari szabványokra vonatkozó kérdéseket.

5.3.1 A személygépjármű mint IoT eszköz

Ennek a kérdésnek a relevanciáját az adja, hogy a személygépjármű, illetve annak alkatrészei hasonlítanak az IoT-ként definiált eszközökre és az ezekre vonatkozó szabályozási környezet jelenleg még szintén igen hézagos – így van létjogosultsága az olyan javaslatoknak, mint például hogy az IoT eszközök esetében megjelenő új szabványokat a személygépjárművek esetében is alkalmazzák az auditorok.

A kutatás során megkérdezett szakértők mindegyike egyöntetűen IoT eszközként tekint a személygépjárműre információbiztonsági szempontból. Ezt javarészt azzal indokolták, hogy a jármű a szenzorok által adatokat rögzít és a külső hálózattal is képes a kommunikációra. Az egyik interjúalany megközelítése a többiekhez képest egyedi volt abban, hogy felvetése szerint nem maga a jármű tekinthető IoT eszköznek, hanem annak alkatrészei. Ezt a megközelítést támasztja alá a személygépjármű, mint kiberfizikai rendszer komplex összetétele és alkatrészeinek sokfélesége.

Azonban ha a személygépjárművet ilyen nézőpontból vizsgáljuk azzal azt kockáztatjuk, hogy egyes alkatrészek kimaradnak az ellenőrzésből. Az egyik interjúalany a korábban bemutatott ISO/SAE 21434 szabvánnyal kapcsolatban kiemelte, hogy bár az jelentős változással kecsegtet a személygépjárművek elektronikai biztonságát tekintve, mivel az egyes elemekre fókuszál a teljes rendszer helyett, ezért nem nyújt teljes megoldást. Amennyiben tehát az IoT eszközökre érvényes szabványokat kívánjuk alkalmazni a személygépjármű egyes részeire, akkor ezt a lefedettséggel összefüggő kockázatot figyelembe kell vennünk.

5.3.2 Kockázatelemzés, metrikák, adatbiztonság

A teljes mintából egy szakértő nyilatkozta csupán, hogy szerinte az ISO 27001 (és ISO 27005) elvárásai alapján végzett kockázatelemzés – megfelelő módon alkalmazva – képes biztosítani a végfelhasználó adatainak biztonságát. Véleményét azzal indokolta, hogy mivel a szabvány kimondja, hogy a szervezetnek a rá vonatkozó jogszabályoknak meg kell felelnie, így nem csak a szabvány követelményeinek való megfelelés, hanem a NIS2 vagy a GDPR-nak való megfelelési kötelezettség is biztosított az Európai Unió területén.

A másik kilenc interjúalany véleménye azonban ettől markánsan eltér, többnyire az elmélet és a gyakorlat között tátongó különbségekre hívják fel a figyelmet, illetve arra, hogy a szabványok betartásának kikényszerítésére nincsenek megfelelő eszközök.

Példaként említik, hogy a beszállítók kibújhatnak a megfelelés alól azzal, ha például azt nyilatkozzák, hogy egy adott szabvány bevezetése már folyamatban van, míg végül a minősítő auditra évek múltán sem kerül sor. A szakértők olyan esetről is beszámoltak, amikor egy szabvány adatbiztonságra irányuló követelményeinek való megfelelést a tanúsítást kérő szereplő egyszerűen egy ügyvédi iroda által kiállított nyilatkozattal oldotta meg.

Akkor sincs biztosítva azonban a megfelelés, ha minden szereplő megfelelő hozzáállással rendelkezik, hiszen a legtöbb kockázatkezelési módszertan – függetlenül attól, hogy specifikusan a személygépjárműiparra vagy egyéb gyártási területre vonatkozik-e – nem írja elő, hogy a maradványkockázatokat milyen időtartam alatt kell kiküszöbölni, hanem az erre vonatkozó szabályok és gyakorlatok pontos kidolgozását a szervezetre hagyja.

5.3.3 Kihívások és megoldási javaslatok

A kihívások kapcsán több interjúalany is kiemelte a jármű, mint végtermék komplexitását. Két interjúalany is rávilágított arra, hogy egyre nagyobb kihívást fog jelenteni a személygépjárművek szoftverkörnyezetének támogatása. Amennyiben a szoftvertámogatás lejár, akkor onnantól kezdve nem biztosított a megfelelő védelem sem, és erre a jelenleg elterjedt kockázatkezelési módszertanok sem tudnak megoldással szolgálni sem az autóiparban, sem az IoT eszközöket gyártó szervezetekkel kapcsolatban. Az adatbiztonság szempontjából, ahogyan az IoT eszközök esetében is, kihívásnak tekinthető az is, hogy a felhasználó nem kap rálátást arra, mi történik pontosan a személyautó informatikai rendszerével és adataival egy szerviz során. Ezt nem csak megfelelő tájékoztatással, de egyes interjúalanyok szerint kifejezetten erre a célra szolgáló archiválóeszközökkel kell biztosítani, azaz lényegében egy az aviatikában is ismert fekete doboz használatára lenne szükség.

Az egyik interjúalany arra világított rá, hogy a Common Criteria szabvány széleskörűbb alkalmazása megoldást jelenthetne a személygépjárművek információbiztonságának termékalapú megközelítésére, azonban ha a szabvány hivatalos weboldalán felsorolt

biztosított eszközök listáját megnézzük[14], akkor látható, hogy világviszonylatban csak kevés számú eszköz rendelkezik ezzel a minősítéssel. Ezek nagyrésze pedig valamilyen általános informatikai eszköz például tűzfal.

Az ISO/IEC 21434 szabvány esetében már valóban egy iparágspecifikus szabványról beszélhetünk, azonban nem maga a személygépjármű képezi a vizsgálat objektumát, hanem annak egyes elektronikai részei. Ilyenek lehetnek például a fékeket vezérlő elektronikai alkatrészek, de egy *infotaintment* rendszer *bluetooth* modulja is. A személygépjármű biztonságának szempontjából problémát jelent, hogy nem is minden alkatrésszel kapcsolatban várható el a tanúsítás, így viszont a gyártó igényeitől függően csak „foltszerűen" érvényesül annak hatása. Ez ráadásul nem csak a menedzsment szemléletéből, hanem a szűkös erőforrásokból is fakad, hiszen a szigorú előírásoknak való megfelelés magas költségekkel járhat.

Az átfogó megoldási javaslatok tekintetében szinte minden szakértő egyetértett abban, hogy szükséges lenne egy egységes európai szintű jogszabályra, mely pontosan előírja azoknak a kontrolloknak az alkalmazását a személygépjárműgyártók és beszállítói számára, amik jelenleg a szabványokban szerepelnek. Ehhez kapcsolódva szükségessé válik egy olyan hatóság létrehozása is, amely betartatja a szabályokat. Az egyik interjúalany kitért arra is, hogy amíg a gazdasági tényezők nem ösztönzik a gyártókat a nagyobb körültekintésre, addig a helyzet változatlan marad.

A megoldási javaslatok között több szakértő ötletei között szerepelt egy átfogó, egész fejlesztési életciklust lefedő és az összes szereplőre kiterjedő kockázatelemzési megoldás bevezetése egy már alkalmazott szabvány keretén belül. Az egyik szakértő az ISO 26262-t emelte ki, melynek jelenleg is szerves részét képezi a kockázatelemzés (ISO 26262-3). Az ISO 26262 funkcióalapú megközelítést alkalmaz, ami miatt nincs szükség a járműelemek részletes ismeretére, így az ipari titok védve marad. Az ISO 26262 kockázatelemzési elvárásai részletesek és a keretrendszere jól átgondolt, azonban a kiberbiztonságra nem fektet elég nagy hangsúlyt, ami abból is látszik, hogy a klasszifikációs rendszerében kifejezetten a sérülésekre fókuszál – így az adatokkal való visszaélés nem jelenik meg közvetlenül benne. További probléma, hogy a szabvány még nem megfelelően elterjedt. Ugyanez a szakértő szintén kiemelte a ISO/SAE 21434 szabványt is, mely az ISO 26262-vel szemben kifejezetten az információbiztonságra

[14] https://www.commoncriteriaportal.org/products

fókuszál és kockázatmenedzsment rendszere kiterjedtebb, azonban nem domborítja ki kellőképpen az ellátási lánccal kapcsolatos elvárásokat és a személygépjármű komplex mivolta, illetve amiatt hogy ugyanúgy túlzottan sok részletet bíz a gyártóra, mint a többi szabvány nem képes hatékony megoldást kínálni. Az ISO 21434 alkalmazásánál például – egyébként más, korábbi szabványokhoz hasonlóan – az információ védelmére elegendő kockázatkezelési módszer a titoktartási szerződések használata – ami azonban a gyakorlatban sajnos nem véd eléggé a támadók ellen. Emiatt a kockázatelemzési elvárásokat tovább kellene szigorítani.

Az interjúalanyok összességében nem tudtak olyan IoT eszközökre vonatkozó szabványokról beszámolni, amelyek megoldanák a fenti, autóiparra vonatkozó kihívásokat, viszont elismerték, hogy ezek a kihívások a két terület között nagyon hasonlóak, így a jövőben mindenképpen szükség lenne a szinergikus szabályozás kialakítására.

Végül a tíz interjúalanyból három is megoldási javaslatként hivatkozott a felhasználók tudatosságának növelésére. Az interjúalanyok általános vélekedése szerint ugyanis a felhasználót többnyire magát sem érdeklik az információbiztonsági problémák, csak akkor, ha egy eszköz meghibásodik vagy az adataik valóban veszélybe kerülnek, kiszivárognak. Ezzel kapcsolatban sokszínű megoldási javaslatok születtek az általános iskolai edukációtól (például információbiztonsági előadások az informatika órán) kezdve az átláthatóbb tájékoztatószövegek átadásáig.

Egy olyan vélemény is akadt, melynek lényege egyenesen az volt, hogy a fejlett kényelmi és szolgáltatási célú eszközök, gyakorlatok alkalmazását, mint például az ülésfűtés szolgáltatásként való nyújtását, be kéne tiltani a személygépjárművekkel kapcsolatosan. Ennek a gondolatnak a logikai hátterét az adja, hogy az informatika fejlődése ma már olyan méreteket ölt, hogy ennek köszönhetően a biztonsági szakemberek és a szabványok semmiképpen nem tudnak lépést tartani vele.

5.4 Összegzés

Összességében a kutatás alapján elmondható, hogy az IoT eszközök szabályozási kihívásai nagyon hasonlóak a személyjárművekkel kapcsolatos kihívásokhoz, azonban a személygépjárműiparra vonatkozó szabályozási környezet valamivel fejlettebb, mint az IoT eszközökre vonatkozó általános szabályozások tartalma.

A vizsgálat során bemutatott szabványok és jogszabályi környezet elsősorban a gyártókat védik, folyamatközpontú és még az olyan célzott szabályok ellenére is, mint a GDPR, kevés hangsúly jut a végfelhasználó adatinak biztonságára. A szabványok nagy része folyamatalapú, a termékközpontú szabványokat pedig a jármű egyes részeire alkalmazzák csak, illetve az ellátási lánc vizsgálatának elterjedtsége is alacsony mértékű.

A vizsgálat során azt tapasztalhattuk, hogy az interjúalanyok megerősítették és többféle különböző aspektusból is rávilágítottak arra, hogy a személygépjárművekben keletkezett vagy használt adatok biztonságának szabályzása és a folyamatok megfelelő biztosítása kihívást okoz a szakemberek számára. A szabályozási környezet az információbiztonság területén töredezett, sok esetben túlzottan megengedő és ennek megfelelően nem hatékony.

Kiderült, hogy a szakértők véleménye meglehetősen sokrétű, többen többféle oldalról közelítik a megoldást. Összességében elmondható azonban, hogy a vélemények többsége kettéoszlik: a szakértők a legnagyobb problémát egyrészt a szabványok gyakorlati betartatásában, a megfelelő minőségű és részletességű kockázatkezelési módszertan hiányában, a megfelelő erővel bíró hatóság hiányában látják, másrészt pedig a felhasználók attitűdjében, tudatosságuk hiányában.

A fejezet eredményei alátámasztják a H4 hipotézist, miszerint a személygépjárművek adatbiztonságának megerősítéséhez szükség van átlátható adattovábbítási rendszerre, titkosított adatforgalomra és megfelelő hatósági felügyeletre. Az IoT eszközök definíciói és a személygépjárművek technológiai jellemzőinek összehasonlítása rávilágított arra, hogy a jelenlegi autóipari szabályozások az átfogó IoT-biztonsági megközelítések adaptálásával továbbfejleszthetők lennének. Az IoT szabályozási környezet kihívásai és fejlődése egyaránt azt jelzi, hogy a járművek hatékony védelme érdekében olyan szabályozásokra van szükség, amelyek a járműveket egységesen kezelik az adatbiztonsági folyamatokban, így biztosítva a felhasználói adatok védelmét és a biztonságos adatkezelési gyakorlatok kialakítását.

A fejezet eredményei alátámasztják a H5 hipotézist, mivel a szakértői vélemények és az interjúk elemzése egyértelműen rávilágít arra, hogy a jelenlegi szabályozási környezet nem elég átfogó a személygépjárművek adatbiztonságának teljes körű biztosításához. A kockázatkezelés egyes elméleti alapelvei, mint például az ISO 27001, ISO 26262 és az ISO 21434 szabványok, nem fedik le teljes mértékben a járművek kiberbiztonságához

szükséges gyakorlati lépéseket. Az átfogóbb, az ellátási láncra is kiterjedő, részletes kockázatkezelési megközelítés, amely minden adatkezelési aspektust figyelembe vesz, hozzájárulhat a járművek fokozott biztonságához, a felhasználók jobb tájékoztatásához és a szabályozási hiányosságok pótlásához. A kockázatértékelés során figyelembe kell venni a támogatási időt és garanciát is.

Elmondható, hogy a javasolt megoldások túlmutatnak az információbiztonsági szabályozási intézkedések hatókörén, azonban ettől függetlenül is fontos alapot jelenthetnek mind a további felhasználói attitűdvizsgálatok, mind pedig a szabályok betartásának lehetséges megoldási módjait kereső kutatások számára.

6. MODELLEZÉS – EGY KOCKÁZATI TÉNYEZŐ VIZSGÁLATA

A modern autóipar átalakulása és az intelligens technológiai megoldások integrálása az autókat összetett informatikai rendszerekké alakította, amelyek folyamatos adattovábbításra és hálózati kapcsolatokra épülnek. Ez a fejezet a H2 hipotézist vizsgálja, miszerint a személygépjárművek, mint egységes informatikai eszközök, ki vannak téve a hackertámadásoknak, vonzó célpontnak számítanak és lehetőséget biztosíthatnak a titkos adatküldésre a felhasználó és a gyártó tudta nélkül. A fejezet a telematikai rendszerek, a kommunikációs protokollok és az MQTT alapú rejtett csatornák sebezhetőségeit és azok kihasználhatóságát elemzi. Az MQTT (Message Queuing Telemetry Transport)[15] egy egyszerű *„publish-subscribe”* modellen alapuló kommunikációs protokoll, amelyet alacsony sávszélességű és korlátozott erőforrásokkal rendelkező eszközök közötti adatátvitelre terveztek. Eredetileg olajvezetékek távoli megfigyelésére fejlesztették ki, de mára az IoT világában vált széles körben használt szabvánnyá. Az MQTT egy központi brókert használ, amely kezeli az üzeneteket a kliensek között: egyes eszközök (publisherek) üzeneteket küldenek egy adott témakörhöz (topic), míg más eszközök (subscriberek) feliratkoznak ezekre a témákra, és megkapják az információkat. Az alacsony késleltetés és a minimális hálózati forgalom miatt ideális megoldás érzékelők, okosotthon-eszközök és ipari alkalmazások számára.

A cél annak bemutatása, hogy a személygépjárművek adattovábbítási képességei, különösen az egyre elterjedtebb MQTT protokoll révén, olyan biztonsági kockázatot

[15] https://mqtt.org

rejthetnek, amely lehetővé teszi akár a felhasználó, sőt a gyártó által sem ismert adatküldést is.

A modern okosjárművek adatbiztonságával kapcsolatos kockázatokra világít rá egy nemrégiben megjelent riport, amely szerint a Tesla egyes dolgozói hozzáférhettek a járművek fedélzeti kamerái által rögzített, titkosítatlan képekhez, és azokat saját célra meg is osztották egymással. Az esetről a Reuters beszámolójában olvashatunk, amely szerint a munkavállalók számára elérhetővé váltak érzékeny tartalmú felvételek – többek között olyan, otthonokban készült privát képsorok, amelyek nemcsak az autók közvetlen környezetét, hanem egyes tulajdonosok személyes életterét is rögzítették. Különösen figyelemre méltó egy eset, amely során egy jól felismerhető, egyedi csónak jelent meg a felvételen, amelyet a beszámolók szerint Elon Musk birtokában lévőként azonosítottak. Ez a példa azt sugallja, hogy a járművek által generált adatforgalom egy része ellenőrizetlenül kerülhet harmadik felekhez, és maga a gyártó sem mindig képes szigorúan szabályozni, hogy ki férhet hozzá az érzékeny információkhoz. A riport szerint a dolgozók több alkalommal egymás között osztottak meg ilyen adatokat, megkerülve ezzel az adatvédelmi előírásokat és komoly kockázatokat idézve elő a felhasználók magánéletére nézve. [94]

Bár a riportok alapján feltételezhetjük, hogy az autókból érkező adatok nem minden esetben titkosítottak, ezt tudományosan még nem bizonyították meggyőzően. Éppen ezért a jelen tanulmány a gyártói és felhasználói felelősségre koncentrálva azzal a feltételezéssel él, hogy az adatok titkosítva kerülnek feldolgozásra, és csak engedélyezett felek számára hozzáférhetők. Ugyanakkor az olyan komplex és szerteágazó adatáramlás védelme, amelyet a modern okosjárművek működését jellemzi, kihívást jelent a gyártók és adatfeldolgozó cégek számára is. Így még az ismert adatbiztonsági mechanizmusok feltételezett alkalmazása mellett is fennáll a lehetősége annak, hogy egyes jól felkészült gazdasági háttérrel rendelkező vagy állami hackercsoportok vagy kormányzati szereplők rejtett csatornákon keresztül képesek lehetnek hozzáférni az adatokhoz anélkül, hogy erről a felhasználók vagy akár maguk az adatkezelők értesülnének.

A kortárs autóiparban a járművek dinamikus adatközpontokká alakultak, mozgó adatközpontokként funkcionálnak. Ezt az átalakulást a fedélzeti Dolgok Internete (Internet of Things, IoT) szenzorok és kifinomult számítástechnikai egységek integrációja hajtja, melyek célja a jármű működésével kapcsolatos létfontosságú információk gyűjtése

és feldolgozása [97]. Ezen technológiai fejlesztések egy olyan korszakot nyitottak meg, ahol az autók összetett hardverek, bonyolult szoftverek és összetett IoT eszközök összefonódásából állnak – amelyek mind együttműködve széles körű szolgáltatások nyújtására képesek.

Az MQTT (Message Queuing Telemetry Transport) protokoll egy olyan kis erőforrásigénnyel rendelkező üzenetküldési protokoll, amelyet kifejezetten az IoT (Dolgok Internete) eszközökhöz, alkalmazásokhoz terveztek.

Az okos járművek megjelenésével számos tanulmány foglalkozott már a modern autók sebezhetőségeinek vizsgálatával, ezzel együtt az MQTT protokoll rejtett csatornaként való alkalmazásával is [96], [97], [98], [99]. A protokoll szerkezetileg az kiadó-feliratkozó (publisher-subscriber) modellt követi, amelyet korlátozott hálózati sávszélességű környezetekre terveztek, ahol a távoli eszközök hálózati korlátokkal néznek szembe. Bár az MQTT használata kézenfekvő lehet az okosjárművek adatcseréje során, jelentős hiányosságok figyelhetők meg a működésében: kevés átfogó tanulmány készült, amely egyesíti ezt a két aspektust. Különösen kevés a tudományos információ arra vonatkozóan, hogy az autók, amelyek mobil és potenciálisan életveszélyes eszközök, hogyan válhatnak sebezhetővé biztonsági résekkel szemben az MQTT protokoll rejtett felhasználása révén. Ezen két kritikus terület – a járműbiztonság és az MQTT-alapú rejtett csatornák kihasználása – összefonódása nagyrészt feltáratlan maradt, amely ígéretes kutatási irányt kínál.

Ahogyan a korábbi fejezetekben bemutattam, a személygépjármű mint összetett termék bonyolultsága miatt az információbiztonsági intézkedések alapvető kockázatelemzésének végrehajtása különösen nehéz [100]. A minden szereplő számára kötelező auditok és biztonsági ellenőrzések hiánya, mind a gyártói, mind a beszállítói szinten, fokozza az autóipari ökoszisztéma potenciális sebezhetőségeit [101].

A modern járművekből származó adatfolyamok olyan információözönné fejlődtek, amely a gyártók és harmadik feles szolgáltatók felhőalapú adattáraiba áramlik, hogy további feldolgozás során értékes megállapításokat nyerhessenek ki belőlük például a fejlesztésekhez vagy az értékesítéshez. Ezen adatok nemcsak a jármű működési paramétereit tartalmazzák, hanem betekintést nyújtanak a vezetők viselkedésébe, szokásaiba és preferenciáiba is. Az olyan vállalatok példái, mint a Tesla, amelyek kiterjedt valós idejű adatokat gyűjtenek járműveikről, megmutatták, hogy ezt az

információt fel lehet használni olyan célokra, mint a jármű teljesítményének optimalizálása, távoli frissítések, sőt, a fejlett vezetéstámogató rendszerek (ADAS) fejlesztése [102]. Ugyanakkor nem hagyható figyelmen kívül az a lehetőség, hogy ezeket az adatokat megfigyelési célokra is felhasználhatják. Az utóbbi idők eseményei, például a kínai kormányzati épületek megfigyelésére vonatkozó adatfelhasználási viták, kérdéseket vetnek fel azzal kapcsolatban, hogy a modern személygépkocsik mennyire válhatnak akaratlanul is a megfigyelés eszközeivé [103].

6.1 Telematikai eszközök és adattovábbítás

Az autóipari telematikai adatokra vonatkozó elemzések az utóbbi időben jelentős figyelemnek örvendenek, bár tudományos minőségű publikáció – érthető okokból – kevés született a témában. Az internetkapcsolatra képes személygépjárművek folyamatosan szolgáltatnak adatokat a belső működésükről, például a sebességről, a helyzetükről vagy a karbantartási igényeikről. A telematikai adatok [104] széleskörű információkat foglalnak magukban, amelyeket a járművek információs rendszerei gyűjtenek. A telematikai adatok kulcsfontosságú eszközként szolgálnak az egyes vezetők mobilitási mintáinak részletes megismeréséhez. Ezen információk valós idejű elemzése lehetővé teszi a biztonság növelését, a költségek csökkentését vagy a járművek teljesítményének javítását.

Bergman és munkatársai tanulmányukban [104] a gyorsulási adatok elemzésére fókuszáltak egy svájci autókereskedés kontextusában. Az elemzett adatkészlet 2019 és 2021 között gyűjtött sebességadatokból állt. Az elemzés célja az volt, hogy a termékkínálatot jobban az egyéni vásárlói igényekhez igazítsák különös tekintettel arra, hogy azonosítsák a különböző modellek és típusok tipikus és atipikus használati mintáit. Ez az alapvetően funkcionális célokat szolgáló vizsgálat szorosan összefügg a vezetői viselkedés megismerésével, amit a telematikai adatok elemzése tett lehetővé. Azok az ügyfelek, akik beleegyeztek személyes adataik feldolgozásába, lehetőséget biztosítottak a gyártónak a részletesebb vásárlói profilok létrehozására. Minden egyes vezető adatkészlete körülbelül 50 000 adatpontot tartalmazott, ami lehetővé tette vezetési viselkedésük mélyreható elemzését és vizualizációját. A profilokat használva az értékesítési munkatársaknak alaposabban kidolgozott ajánlatok adására lettek képesek a jövőbeli járművásárlások során. A tanulmány megállapította, hogy a telematikai adatok felhasználhatók a vezetői viselkedési szokások és az általános járműhasználat

megismerésére, amely végső soron az autóipar és egyes esetekben a felhasználó (személyre szabottabb ajánlatok) javát is szolgálja.

Annak ellenére, hogy egyre több telematikai megoldás érhető el, a gépi tanulási modellekre épülő élő rendszerek alkalmazása még viszonylag korlátozott. Figyelemre méltó, hogy a biztosítási ágazat már integrálta a telematikai adatokat, és alapként használja őket a használatalapú biztosítási díjak kiszámításához. Az ilyen és ehhez hasonló felhasználási területek növekvő jelentősége miatt egyre több kutatás [105], [106] mutatja be a telematikai adatkezelés gyakorlati alkalmazását az autóiparban, rávilágítva arra, hogyan lehet ezeket az adatokat a vásárlói profilozás javítására és a termékkínálat finomhangolására felhasználni. Ez alátámasztja az adatalapú megállapítások növekvő jelentőségét, amelyek az autóipar jövőjét formálják.

A modern személygépjárművek különböző protokollokon keresztül kommunikálnak internet-hozzáféréssel rendelkező szerverekkel, lehetővé téve az adatok cseréjét a jármű fedélzeti rendszerei és külső egységek között. Ezek a protokollok gyakran magukba foglalják a HTTP (Hypertext Transfer Protocol) és a HTTPS protokollokat (Hypertext Transfer Protocol Secure) a webes alapú kommunikációhoz, lehetővé téve a járművek számára, hogy biztonságosan küldjenek és fogadjanak információkat az interneten keresztül. Emellett az MQTT (Message Queuing Telemetry Transport) gyakran használt megoldás az adatok hatékony és könnyű átvitelére, amely ideális a valós idejű monitorozáshoz és irányításhoz, mivel nagyon kicsi erőforrást igényelnek és egyszerűek. Ezek a kommunikációs protokollok kulcsszerepet játszanak abban, hogy az adatok zökkenőmentesen áramoljanak a járművek és a távoli szerverek között, támogatva olyan funkciókat, mint a távoli diagnosztika, szoftverfrissítések, felhőalapú elemzések és még sok más. Azonban ahogy az átvitt adatok köre és érzékenysége bővül, a kommunikációs csatornák biztonságának és adatvédelmének biztosítása egyre kritikusabbá válik.

A. Ullah és munkatársai [105] egyik tanulmányukban az internethez kapcsolódó járművek világának növekvő térnyerését és az azzal járó biztonsági és megbízhatósági kihívásokat vizsgálták. A tanulmány feltárja a járművek közötti (V2V) és a jármű-infrastruktúra közötti (V2I) kommunikációban használt protokollokat és architektúrákat, rávilágítva a rendszerben rejlő potenciális sebezhetőségekre és fenyegetésekre. Bár az értekezésem fókusza alapvetően a ma elterjedt személygépjárművek működése és nem a jövőbeli, infrastruktúrával és egymással kommunikáló járműveké, azáltal, hogy

megvilágítja a lehetséges megoldásokat és kihívásokat, ez a kutatás alapvető betekintést nyújt a modern járműkapcsolatokhoz szükséges kommunikációs protokollok megértéséhez. S. Kumari és munkatársai [106] átfogó áttekintést nyújtanak az IoT (Dolgok Internete) konnektivitás paradigmájáról a járművek kontextusában. Ez a kutatás a járműhálózatokban alkalmazott IoT elvek integrációját vizsgálja, hangsúlyozva a közvetített adatok sokféleségét, beleértve a biztonságkritikus információktól kezdve az infotainment adatokig. A tanulmány értékeli a használt kommunikációs protokollokat, mint a HTTP, MQTT (Message Queuing Telemetry Transport) és CoAP (Constrained Application Protocol), valamint foglalkozik az érzékeny járműadatok átvitelében rejlő biztonsági és adatvédelmi kihívásokkal.

Ezek a vizsgálatok értékes betekintést nyújtanak a jármű-adatátvitelhez kapcsolódó protokollok, architektúrák, sebezhetőségek és potenciális megoldások tekintetében. Ahogy az autóipar tovább fejlődik, ezek a kutatási eredmények szilárd alapot nyújtanak az internetkapcsolatra képes járművek biztonságának és adatvédelmének fokozására irányuló stratégiák kidolgozásához. Különösen érdekes annak feltárása, hogy az MQTT hogyan emelkedett ki az autóiparban. Számos eredeti berendezésgyártó (OEM) és beszállító már régóta kínál csatlakozási megoldásokat járműveiben. Az elsőgenerációs csatlakozási megoldások gyakran az SMS-re (Short Message Service) és a HTTP-re (Hypertext Transfer Protocol) támaszkodtak. Ezek a technológiák azonban nem voltak célzottan úgy kialakítva, hogy megfeleljenek az okosautók igényeinek. A HTTP például állandó hálózati kapcsolatot igényel, miközben a járművek a mobilhálózatok segítségével osztják meg az adatokat, amelyek – főleg mozgás közben – nem nyújtanak megbízható kapcsolatot. Az SMS sem képes azt a valós idejű üzenetküldési funkciót nyújtani, amely elengedhetetlen a modern autószolgáltatások zökkenőmentes működéséhez. Az autó ajtajának SMS-sel és HTTP-vel történő kinyitása például több mint 30 másodpercet vesz igénybe, ami nyilvánvalóan elfogadhatatlan a mai fogyasztók számára, akik az azonnali reagálást várják el a digitális interakció során. Továbbá az SMS és a HTTP jelentős hálózati sávszélességet igényelt, ami miatt rendkívül költséges megoldásnak bizonyultak. Az MQTT protokoll ezért ideális megoldást jelent a kapcsolt autók számára, amit részletesen elemzett például a HiveMQ is [107].

6.2 A rejtett csatornák (Covert Channels) elméletének alkalmazása a titkos információküldés vizsgálata során

A rejtett csatornák (covert channels) elemzése a informatikai biztonság és a hálózatbiztonság egyik speciális területe. A "rejtett csatornák" fogalmának keletkezése a 20. század közepéig nyúlik vissza, amikor a számítógépek és digitális rendszerek fejlődése megkezdődött. A rejtett csatornák kutatásának első úttörői amerikai katonai és hírszerzési szakemberek voltak a hidegháború időszakában. Az 1970-es évek végén és az 1980-as évek elején a rejtett csatornák kutatása egyre nagyobb jelentőségre tett szert a számítógépes biztonság és a hírszerzési tevékenységek területén. Ebben az időszakban alakultak ki az első módszerek és technikák a rejtett kommunikáció felismerésére és az ilyen csatornák használata elleni védekezésre a számítógépes rendszerekben [108].

A rejtett csatornák elemzésének elsődleges célja azon rejtett vagy titkos kommunikációs mechanizmusok azonosítása és elemzése, amelyeket rosszindulatú szereplők alkalmazhatnak információk jogtalan továbbítására vagy titkos tartalmak elrejtésére. Ezen csatornák azáltal jönnek létre, hogy a szándékolt és engedélyezett kommunikációs utaktól eltérő módon használják a kommunikációs technológiákat, gyakorlatilag kihasználva a rendszer vagy hálózat különböző működési aspektusait vagy sebezhetőségeit. Ennek következtében nehezen észlelhetők, és lehetőséget teremthetnek olyan tevékenységekre, mint az adatszivárogtatás vagy jogosulatlan rendszerhozzáférés.

A rejtett csatornák elemzésének területén a kutatók és a kiberbiztonsági szakemberek arra törekednek, hogy feltárják és dokumentálják az ilyen titkos kommunikációs mechanizmusokat, továbbá védelmi stratégiákat és eszközöket fejlesszenek ki azok kockázatainak csökkentésére. Végső céljuk megérteni, hogy az egyes csatornák miként működnek, és olyan intézkedéseket kialakítani, amelyek lehetővé teszik azok megelőzését vagy felismerését a számítógépes rendszerekben és hálózatokban. Ennek köszönhetően a rejtett csatornák elemzése kulcsszerepet játszik az információbiztonságban, célja, hogy azonosítsa és megszüntesse a rejtett és jogtalan kommunikációs mechanizmusokat a számítógépes rendszerek és hálózatok integritásának és titkosságának megőrzése érdekében.

Az egyre növekvő adatcserével a személygépkocsik és a telekommunikációs hálózatok között, ahol az adatok az interneten keresztül különböző érdekelt felekhez jutnak el,

különösen fontossá válik a különböző hálózati rétegek biztonságának megőrzése. Az 5G megjelenésével a „biztonság tervezés által” központi szemponttá vált a szabványok létrehozói számára, modern eszközöket integrálva a hálózati rétegek megerősítésére (ám a sokféle beállítás és a rugalmas programozhatóság potenciálisan kihasználható lehet) [109]. Ezen erőfeszítések ellenére a népszerű protokollok, mint például az MQTT, nem mutattak jelentős biztonsági előrelépéseket a legújabb verzióikban, még az MQTT v5-ben sem. Ennek következtében téves feltételezés lenne azt hinni, hogy az 5G hálózatok önmagukban garantálják a járműkommunikáció adatbiztonságát, mivel a protokollok továbbra is sebezhetőségeket mutathatnak [110].

Elemzésem során Velinov és munkatársai [111] kutatásaira építettem, akik alaposan megvizsgálták az MQTT-alapú rejtett csatornákat, és 16 ilyen csatornát (azaz kihasználási lehetőséget) azonosítottak az MQTT protokollon belül. A kutatásukban vizsgált MQTT-alapú rejtett csatornarendszer modellje egy rejtett küldőt (CS – covert sender) és egy vagy több rejtett vevőt (CR – covert receiver) foglal magában. Fontos megjegyezni, hogy a modell több rejtett küldő bevonódását is lehetővé tesz, noha jelen tanulmány elsősorban egyetlen CS-re összpontosít. Ezenfelül az MQTT eredendő sokoldalúsága bármely kliens számára lehetővé teszi a kiadó (publisher) szerepének betöltését, elősegítve a kétirányú kommunikációt és a csoportos alapú kommunikációt a felhasználók között. Ez az alkalmazkodóképesség lehetővé teszi, hogy a CS és a CR-ek ugyanazon a hálózaton belül vagy különböző hálózatokon keresztül működjenek. Velinov és munkatársai [111] megkülönböztetést vezetnek be két specifikus almodell között: a Direkt Rejtett Csatornák (DCC) és az Indirekt Rejtett Csatornák (ICC) almodellt. A Direkt Rejtett Csatornák (DCC) almodelljében a CS közvetlenül kommunikál a CR-ekkel, két különböző lehetőséget kínálva: a bróker vagy CS-ként szolgál (DCCa), vagy kizárólag a CR szerepét tölti be (DCCb). Ezzel szemben az Indirekt Rejtett Csatornák (ICC) almodellben a CS közvetett kommunikációt folytat a CR-ekkel a bróker közvetítői szerepén keresztül. Ez a konfiguráció kizárja a CS és a CR-ek közvetlen interakcióját, lehetővé téve az aszinkron rejtett küldési és rejtett fogadási folyamatokat. Ebben a forgatókönyvben a bróker proxy csomópontként működik, továbbítva bármelyik üzenetet, amelyet kap, miközben a rejtett adatcseréről nem rendelkezik információval.

A rejtett csatornák MQTT-ben különböző protokolljellemzők és üzenettulajdonságok kihasználásával hozhatók létre – néhány gyakori terület, amit vizsgálni lehet:

- Témanevek: Az MQTT a témanevekre támaszkodik az üzenetek útvonalazásához. Rejtett csatornák létrehozhatók információk témanevekbe történő kódolásával, amelyek észrevétlenek maradhatnak, ha nem vizsgálják meg őket alaposan.
- QoS Szintek: Az MQTT-ben különböző QoS szintek (0, 1 és 2) különböző mértékű üzenet-megbízhatóságot biztosítanak. A támadók a QoS szintek variációit használhatják rejtett csatornák létrehozására, ahol az időzítés által kódolhatják az üzeneteket.
- Hasznos információt hordozó adatok (payload): Az MQTT üzenetek valamilyen specifikus információra vonatkozó adatokat, amelyeket manipulálni lehet rejtett adatok továbbítására.
- Megtartott üzenetek: Az MQTT lehetővé teszi az üzenetek megtartását a brokerek által, ami visszaélésre ad lehetőséget.

A fentiek alapján a rejtett csatornaelemzés végrehajtásához a biztonsági szakembereknek a következő lépéseket kell követniük:

- Forgalomfigyelés: Az MQTT protokoll hálózati forgalmának folyamatos monitorozása az anomáliák felismerése érdekében, például szokatlan témaprofilok, üzenetméretek vagy QoS szintváltozások észlelése.
- Terhelésellenőrzés: Az üzenet terheléseinek ellenőrzése rejtett információk vagy szokatlan kódolási technikák jelenlétének felismerése céljából.
- Mintafelismerés: Mintafelismerő algoritmusok alkalmazása gyanús üzenetminták azonosítására, amelyek rejtett csatornák jelenlétére utalhatnak.
- Viselkedéselemzés: Az MQTT kliensek és brokerek viselkedésének elemzése szokatlan kommunikációs minták vagy a várttól eltérő működés kimutatása céljából.
- Biztonsági Szabályzatok: Olyan MQTT biztonsági szabályzatok kidolgozása és betartatása, amelyek meghatározzák az engedélyezett témaszerkezeteket, QoS szinteket és terhelésformátumokat.

Tanulmányomban az eddig bemutatottak közül a hasznos adattartalommal (payload) kapcsolatos rejtett csatornák kihasználásának vizsgálatára összpontosítok. Kifejezetten az MQTT üzenetek tartalmának módosítására helyezem a hangsúlyt, azzal a céllal, hogy

megőrizzük a normál üzenetműködés látszatát, miközben lehetővé teszem egy rejtett üzenet összeállítását a fogadó (feliratkozó) oldalon, amikor a megfelelő minták ismertek. Ez a módszertan a szteganográfia tudományán alapul, amely során egy adatfajtát egy másikba ágyazva rejtenek el, úgy, hogy az adott adattípusban a kivont üzenet észrevétlen maradjon az illetéktelen megfigyelők számára. Emellett a téma nevének megválasztása kulcsszerepet játszik az adatok valódi természetének elrejtésében. Az MQTT témaneveket használ az üzenetek adott feliratkozóhoz történő irányításához. Olyan témanevek megválasztásával, amelyek gyorsulásmérőkhöz vagy más kapcsolódó érzékelőkhöz kapcsolódó összefüggést sugallnak, még akkor is, ha az adatfolyam valójában helymeghatározási adatokat tartalmaz, további obfuszkáció érhető el. Egy „acceleration/sensor01” névvel ellátott téma például azt a benyomást kelti, hogy gyorsulásmérő adatokat továbbítanak a segítségével.

6.3 Az MQTT Protokoll kihasználásának lehetőségei

A téma érzékeny jellege miatt a rendelkezésre álló adatok nem nyújtanak pontos képet a személygépjárművek adatátviteli mechanizmusairól. Ugyanakkor különböző független adatvédelmi szervezetek értékes forrásokat biztosítanak a témában. Caltrider és munkatársai [112] meghatározzák az adatgyűjtés terjedelmét a modern autókban, és annak adatvédelmi és biztonsági vonatkozásait, kiemelve a felelős adatkezelési gyakorlat fontosságát. A modern gépjárművek adatgyűjtési gyakorlatáról és ezen adatok célállomásairól a Mozilla Foundation weboldalán 2023-ban jelentek meg publikációk a „Privacy Not Included” projekt részeként. [112] A vizsgálatban a kutatók többek között azt tárták fel, hogy az autók hogyan gyűjtenek különféle típusú adatokat – például helymeghatározás, vezetési szokások, infotainment rendszer használata – több forrásból, mint szenzorok, GPS, kamerák és fedélzeti számítógépek. Az adatokat gyakran továbbítják az autógyártók szervereire vagy harmadik felekhez, ami adatvédelmi kérdéseket vet fel. A Mozilla kiemeli, hogy a legtöbb autógyártó adatvédelmi szabályzata homályos megfogalmazásokat használ, így nem egyértelmű, hogy pontosan milyen adatokat gyűjtenek, vagy kivel osztják meg ezeket. A kutatás betekintést nyújt a mai autók által gyűjtött adattípusok megismeréséhez, amelyek közé tartozik a jármű teljesítménye, a helyzet, a vezetési szokások és még a felhasználók interakciói az infotainment rendszerekkel is. Rávilágít arra, hogy ezen adatok különböző forrásokból származnak, mint például szenzorok, GPS rendszerek, kamerák és fedélzeti számítógépek, és hangsúlyozza, hogy az adatgyűjtés nem korlátozódik egyetlen forrásra, hanem a jármű

több összetevőjének szinergiájának eredménye. A kutatás azt is vizsgálja, hogy az autók által összegyűjtött adatok hová kerülnek az adatgyűjtést követően. Rámutat arra, hogy az adatokat gyakran (igaz, többnyire aggregált formában) az autógyártók szervereire vagy harmadik fél szolgáltatóihoz továbbítják, ami adatvédelmi aggályokat vethet fel. Az adatgyűjtés elsődleges céljai között szerepel a jármű teljesítményének javítása, a biztonsági funkciók fejlesztése, valamint kényelmi funkciók biztosítása a vezetők és utasok számára. Emellett azonban kiemeli annak fontosságát, hogy megértsük, milyen mértékben használják fel az adatokat hirdetési és marketing célokra.

A rendelkezésre álló információk és korábbi kutatások alapján több, az okosjárművekre jellemző vagy választható kommunikációs és adatátviteli típust azonosítottam:

- **GPS adatok**: A jármű pozíciójának követéséhez szükséges. Releváns forgalmi információkat csak akkor lehet távolról biztosítani, ha az autó megosztja aktuális helyzetét. Ez az adat számos okostelefon alkalmazásban is tipikus, amikor a felhasználó engedélyezi az alkalmazás számára a GPS használatát.
- **Járműszenzor-adatok**: Az autó összes berendezéséről szolgáltat információt. A motor vagy a fékek hőmérséklete, valamint a gumiabroncsnyomás és számos egyéb belső szenzor rendszeresen jelentést tesz állapotáról, beleértve az esetleges hibaüzeneteket is. Ezek az adatok tárolhatók helyben, de – legalább is aggregált formában – az a tendencia jellemző, hogy távoli szervereken tárolják őket, hogy elkerüljék a tulajdonos általi manipulációt (használt autó értékesítés). Feltételezem, hogy ezek az adatok a közeljövőben ellenőrzött adatbázisokban lesznek tárolva, ami azt is jelenti, hogy folyamatosan továbbításra kerülnek a hálózaton keresztül.
- **Akkumulátorcella-információk**: Elektromos járművek esetén létfontosságú adat. Az akkumulátortechnológia gyors ütemben fejlődik. Az elektromos autó valódi értékét jelentősen befolyásolja az akkumulátor teljesítménye, például a töltési sebesség, fogyasztás, valamint az akkumulátor amortizálódása. Az akkumulátor teljesítményének követéséhez az autónak rendszeresen jelentenie kell az akkumulátor állapotát.
- **Kommunikáció a tulajdonossal**: Az okosautók elvárt funkciója, hogy jelentsenek a tulajdonosnak, ha például az ablak nyitva maradt, vagy ha a riasztó aktiválódott. Ezenkívül a tulajdonos okostelefonos alkalmazásával távolról

bekapcsolhatja például a szélvédő fűtését. Ez távoli kommunikációt igényel egy harmadik fél közreműködésével.

- **Szoftverfrissítés**: A szoftverfrissítés inkább aszinkron kommunikáció. A tulajdonos kezdeményezi a frissítést, és az autó letölti és telepíti az új bővítményeket vagy szoftverfrissítéseket megfelelő hálózati kapcsolat esetén.
- **Biztosítási adatok**: Ez jelentős mennyiségű adat folyamatos továbbítását igényli a vezetési részletekről, például gyorshajtásokról, veszélyes fékezésekről, olyan helyzetekről, amikor az autónak be kellett avatkoznia. Jelenleg az ilyen adatok felhasználása még nem elterjedt.
- **Önvezető funkció adatai**: Az önvezető modul folyamatosan tanul a különböző közlekedési helyzetek elemzéséből. Az önvezető modul által félreértett helyzeteket értékelni kell a szoftver teljesítményének javítása érdekében. Egy ilyen funkció megköveteli, hogy az autó kamerája által készített képeket elemzőszolgáltatóknak továbbítsák, hogy megértsék a képfelismerési hibákat.

Mindezek az adatátviteli megoldások elméleti lehetőséget biztosítanak a támadók számára, hogy a folyamatos információáramlást nemkívánatos kommunikációra használják fel. Ennek tudatában az alábbiakban bemutatott kutatás során különböző lehetőségeket elemeztem, amelyek iránt egy támadó érdeklődhet. A rejtett csatorna sávszélessége alapján a támadó szándéka szerint továbbíthat:

- viszonylag kis mennyiségű információt, például rendszeres adatokat a jármű helyzetéről,
- közepes mennyiségű adatot, például az autó belsejében rögzített hangmintákat,
- nagy mennyiségű adatot, például az autó által készített fényképeket.

Kutatásom az egyes lehetőségek jellemzőinek elemzésére összpontosít, például képek küldésére szenzoradatoknak álcázva. Minden lehetőség esetében feltételeztem, hogy az autó szoftvere kompromittálódott, így a hangsúly kizárólag a rejtett csatornás parancs- és vezérlésmechanizmusokon van, és nem a kibertámadási lánc egyéb részein, mint például a felfegyverzés (weaponization) vagy az exploitáció (exploitation).[113]

A kutatás során az adattudomány módszereit hívom segítségül, hangsúlyozva a képek numerikus reprezentációvá alakításának fontosságát. Ez a transzformáció lehetővé teszi

különböző gépi tanulási technikák alkalmazását, jelentősen javítva a képminőséget. Az ilyen technikák alkalmazásával kiemelkedő eredmények érhetőek el például régi, elmosódott fotók helyreállítása terén, ahogyan azt a [114] referencia is demonstrálja, amelyre támaszkodtunk. Modellkísérletem során feltételeztem, hogy az autó információs rendszere olyan alkalmazással rendelkezik, amely képes egy, a jármű által készített fényképet numerikus adatokra konvertálni. Ezt követően ezeket a numerikus adatokat a szenzorok által generált információkkal együtt egy közvetítőhöz (bróker) továbbítja.

6.3.1 Képi adatok küldése

Kutatásomban egy Star Wars univerzumából ismert fikcionális űrállomás, a Halálcsillag képét alakítottam át numerikus sorozattá, amely tökéletesen rekonstruálható visszafelé is.

Az általam végzett kísérlet során az egyes képpontokat RGB (piros, zöld, kék) értékekkel ábrázoltam. Ezek az értékek hexadecimális formátumban vagy 0 és 255 közötti decimális hármasként fejezhetők ki, lehetővé téve a kép részleteinek pontos rögzítését.

Egy kiváló minőségű fénykép számos képpontból áll. Egy 900 x 1260 képpontos fénykép összesen 1 134 000 képpontot tartalmaz, ami decimális értékben kifejezve 3 402 000 adatpontot jelent.

Kísérleteim szerint egy személy 30 méter távolságból történő azonosításához szükséges CCTV kamera felbontása több tényezőtől függ, beleértve a kép méretét, a lencse minőségét és az azonosításhoz szükséges részletességet. Általánosságban azonban a 1080p (1920 x 1080 képpont) minimális felbontású képfelbontást tartják alapvetőnek a felügyeleti alkalmazások arcfelismerési képességének optimális működéséhez.

Az adatátviteli időt szemléltetve, egy IoT eszköz egy egység adatot generál másodpercenként (például gyorsulási mérések), és az említett adatátviteli sebességgel közel 3 402 000 másodpercre (körülbelül 39 375 napra) lenne szükség ennek az adatmennyiségnek a továbbítására.

A képek pixeltömbként való tárolása nem olyan hatékony, mint a képtömörítés használata, mivel a 39 375 nap igencsak sok idő, a tömörítés alkalmazhatóságát is megvizsgáltam. Egy átlagos JPG kép körülbelül az eredeti méret 90%-ára tömöríthető minimális minőségvesztéssel – azaz úgy, hogy a rajta szereplő személy még felismerhető maradjon.

Egy ilyen JPG kép numerikus sorozattá alakítása hatékonyan képkvantizáció révén oldható meg [115], [116]. Ennek a 10:1 tömörítési aránynak az alkalmazásával egy JPG kép továbbítása körülbelül 4 napot igényelne. Az 50:1 tömörítési arány viszont már olyan minőségromlást eredményezne, amely ellehetetlenítené az arcfelismerést, így ezt a lehetőséget nem vizsgáltuk tovább. Másrészt a JPEG2000 formátum támogatja mind a veszteséges, mind a veszteségmentes kódolást, így alkalmasabb lehet ezen feladatok elvégzésére. Így JPEG2000 esetén nem kell foglalkozni a képminőség romlásával, ugyanakkor a tömörítés hatékonysága emiatt akár rosszabb is lehet. 2019 óta létezik az AVIF formátum, mely a JPG-nél hatékonyabb tömörítést tesz lehetővé, azonban a JPG sokkal elterjedtebb. Kutatásomban a hagyományos JPG kompresszióval számoltam figyelembe véve a képminőség megfelelő megtartását.

Több képtömörítési algoritmus is létezik, amelyek jelentős minőségromlás nélküli tömörítést nyújtanak. Egy GIF kép átlagos aránya körülbelül 4:1, a PNG formátummal pedig a JPG-hez hasonló tömörítési arányt lehet elérni jelentős minőségromlás nélkül. Ezek igénybevételét feltételezve és az időt újraszámolva egy kép továbbítása minőségvesztés nélkül 4 napot venne igénybe.

Másodpercenként egy adategység továbbítása reális lehet a személygépjármű telematikai adatai, például motorhőmérséklet vagy gyorsulási adatok esetén, de kevés lehet nagyobb mennyiségű adatcserére orientált szolgáltatásokhoz, mint például biztosítási autókövetés, fejlett autómonitorozás vagy fejlett vezetéstámogató funkciók. Fejlett autókövetéshez 4 adategységet vettünk figyelembe másodpercenként. Ez az érték azt jelenti, hogy egy képet egy nap alatt lehet továbbítani rejtett csatornán keresztül, ha azt ezt szolgáló célszoftver kompromittálódott.

Mint korábban említettük, az önvezető funkciókhoz rendszeresen kell képeket küldeni a jármű által félreértett közlekedési helyzetek jelentésére. A képek képekbe történő elrejtése sokkal hatékonyabb lehet, mint a képpontok szenzoradatokba rejtése. Figyelembe véve, hogy egy kép 5%-a hasznos adatot tartalmaz, egy rejtett kép 20 másik, félreértett közlekedési helyzetről készült képben küldhető el. Ez jelentősen növeli a rejtett csatornán keresztüli adattovábbítása sebességet, amely gyakori félreértések esetén akár napi több képet is jelenthet.

A legrosszabb esetben az önvezető eszköz egyszerűen félreértett közlekedési helyzetként, hamis megjelöléssel küldheti el a dedikált képet. Ebben az esetben nincs szükség klasszikus értelemben vett rejtett csatornára, csupán szándékosan hamis képfelismerésre.

Képküldés összefoglalása rejtett csatornán keresztül

	Kép mint bitkép	**9x0%-os képtömörítés**
Átlagos telematika	egy kép 40 nap alatt	egy kép 4 nap alatt
Fejlett autókövetés	egy kép 10 nap alatt	egy kép naponta
Önvezető adatok	napi több kép	napi több kép

11. táblázat - A képi adatok rejtett csatornán keresztül történő továbbításának összefoglalása

6.3.2 Hanginformációk továbbítása MQTT rejtett csatornákon keresztül

A digitális hangjelek elterjedtségük és népszerűségük (zenék, hang alapú kommunikációs formák) miatt ideális választássá váltak érzékeny információk továbbítására. Ennek eredményeként a digitális hangszteganográfia jelentős szerephez jutott, különösen a hangalapú adatátviteli technológiák, mint például a VoIP és az audiokonferencia rendszerek rejtett adattovábbításában. A szteganográfiai kritériumok sokfélesége számos rendszertervezési technika létrejöttét eredményezte.

Djebbar és munkatársai [117] tanulmányukban átfogó áttekintést nyújtanak a kortárs digitális hangszteganográfiai módszerekről, és teljesítményüket robusztusság, biztonság és adattárolási kapacitás mutatók alapján értékelik. Ezen túlmenően bemutatják a szteganográfiai modellek osztályozását azok beágyazási folyamatban betöltött szerepe alapján, különös tekintettel a robusztusságra. A vizsgálat különbséget tesz azon módszerek között amelyeknél a rejtett adat mennyisége a fő prioritás (adatrejtési kapacitás) illetve azon módszerek amelyeknél a fő szempont a minél jobb minőségű adatrejtés. A kódolt tartomány módszerei pedig a valós idejű alkalmazásokhoz hasonló kihívást jelentő környezetekben az adatintegritást helyezik előtérbe. A kutatásom során egy ésszerű egyensúlyra törekedtem az átvitt adatmennyiség maximalizálása, a rejtett csatorna minősége és az integritás megőrzése között.

A tanulmány [117] a teljesítményértékelés során az észrevehetőség és a szteganalízis mutatóit vizsgálta. Az eredmények azt mutatják, hogy a frekvenciatartományt gyakrabban választják az időtartománnyal szemben, és a zenei jelek kiváló fedőadatként szolgálnak az adatrejtőképesség, észrevehetetlenség és észlelhetetlenség szempontjából.

Végül a tanulmány hangsúlyozza a meglévő hangszteganográfiai technikák sokféleségét és bőségét, amelyek bővítik az alkalmazási lehetőségeket. Az egyik technika választása az alkalmazási feltételektől függ, beleértve az adat-rejtőképességi kapacitás, adatbiztonság és a potenciális támadásokkal szembeni ellenállás követelményeit.

Mivel a hang kvantálása és a hangszteganográfia összetett számításokat igényel, modellünk egy leegyszerűsített elméleti megközelítést alkalmaz, amely valós példák tanulmányozásán alapul. A modell kidolgozása során figyelembe vettük azokat a meglévő modelleket [118], [119], amelyek a hangadatok kódolására és dekódolására alkalmazott elterjedt módszereket követik, lehetővé téve a hangadat kvantálását és átalakítását oly módon, hogy az maximális hatékonyságot biztosítson a dekódolás során a minőség és a hang tisztaságának megőrzése mellett.

Egy 3 perces hangfájl numerikus értéksorrá alakítása az MQTT protokollon keresztül történő rejtett továbbításhoz, hagyományos numerikus adat formájában, a hang digitalizálását igényli. Ez a folyamat a hangjel gondos, rendszeres időközönként történő mintavételezését és az ezt követő kvantálását diszkrét numerikus reprezentációkba foglalja magába. A hangfájl numerikus adatokká alakítása több kulcsfontosságú lépést igényel. A kompromitált eszköz bármely módon, formátumban is rögzíti a hangmintát ennek WAV vagy PCM formátumba történő konvertálása a preferált, mivel ezek kompatibilisek a digitális manipulációval. A mintavételi ráta kiválasztása, például 44,1 kHz, ésszerű döntés a normál beszéd esetén, mivel ez szabályozza a hangjel mintavételi gyakoriságát. Rejtett hangtovábbításhoz azonban nem feltétlenül szükséges a 44,1 kHz minőség. A mintavételezés során az audiohullámból rendszeres időközönként mintákat veszünk, ahol minden minta a hangjel pillanatnyi amplitúdóját jelzi egy adott időpontban. A kvantálás a következő kritikus lépés. A megfelelő bitmélység megválasztása alapvető fontosságú, mivel ez jelentősen befolyásolja az adatfelbontást. A 16 bites kvantálási séma választása esetén például 65 536 különböző numerikus értéket kapunk. E lépés során egy leképezési eljárás átalakítja a mintavételezett hang amplitúdóértékeit diszkrét numerikus értékekké, amelyek igazodnak a választott bitmélységhez. Ez a komplex művelet a folytonos amplitúdóadatokat kvantált numerikus reprezentációkká alakítja. Ezután a kvantált numerikus adatokat egydimenziós tömbben vagy listában rendezzük el, megteremtve az MQTT hasznos adatok közötti továbbításának alapját. Az MQTT ismertsége révén gazdag funkcionaltású könyvtármodulokkal rendelkezik több

programozási nyelvben is, amely megkönnyíti a támadó dolgát a rejtett adattovábbítás során.

Az eredeti hangfájl visszaállításának fogadó oldali folyamata magába foglalja a kvantálási eljárás visszavonását, amely során a numerikus értékeket visszaalakítják audio mintákká, így lehetővé válik az audiofájl hű visszaállítása. Modellünkben 5 kHz mintavételi frekvenciát alkalmazunk, és egy 3 perces beszédmintát elemzünk. Ezekkel az alapvető paraméterekkel a 3 perces hangfájlt alkotó audio minták összesített száma a következőképpen számítható ki:

Összes minta = Mintavételi ráta x Időtartam

5 kHz szokásos mintavételi rátával:

Összes minta = 5000 minta/másodperc x (3 perc x 60 másodperc/perc)

Összes minta = 900 000 minta

Mivel minden egyes minta 8 biten (16 bites kvantálási séma nem szükséges) kerül meghatározásra (azaz 1 bájt), a teljes adatmennyiség bájtban a következőképpen alakul:

Teljes adat (bájtban) = Összes minta x 1 bájt/minta

Teljes adat = 900 000 bájt

A teljes adatcsomag mérete tehát körülbelül 0,9 megabájt (MB).

Egy adatcsomag továbbítása másodpercenként közel 0,9 megabájtnyi 8 bites adatcsomagot igényelne egy 3 perces hangfájl kódolásához, 5 kHz-es mintavételi frekvenciával és 8 bites kvantálási sémával. Érdemes megjegyezni, hogy ez a számítás egyszerűsített megközelítést képvisel, nem tartalmazza az MQTT csatorna rendes működése által továbbított adatokat vagy a továbbítási folyamat során esetleg alkalmazott további kódolási/tömörítési módszereket.

A képátviteli algoritmushoz hasonlóan hálózatintenzívebb szolgáltatásokat, például fejlett autókövetést is figyelembe vettünk, ahol másodpercenként 4 adategységet küldünk. Ez az eljárás egy 3 perces hangminta továbbításához szükséges időt 3 napra csökkenti.

A legújabb kutatások a hangklónozással kapcsolatban [121] azt mutatták, hogy mindössze 3 másodpercnyi hangfelvétel elegendő valaki hangjának lemásolásához. A hangklónozás a jövőben az egyik legnépszerűbb adathalászati technika lehet, és a

tulajdonos vagy bármely utas hangjának 5 másodperces mintája releváns lehet a támadók számára. Az 5 másodperces hanghossz jelentősen csökkenti a hangminta továbbításához szükséges időt.

Ezenkívül az önvezető funkciók a hibásan felismert közlekedési helyzetek jelentésével hatékonyabbá teszik a hang továbbításának lehetőségeit. A hangminták képekbe való beágyazása jelentősen csökkenti a hangminta továbbításához szükséges időt. A 2. táblázatban összefoglalom a hangadatok továbbításának eredményeit.

	5 másodperces hang	**3 perces hang**
Átlagos telematika	4 óra	10 nap
Fejlett autókövetés	1 óra	2,5 nap
Önvezető	néhány percen belül	néhány órán belül

12. táblázat - Hangadatok rejtett csatornán keresztül történő továbbításának összefoglalása

6.3.3 Helyadatok küldése MQTT rejtett csatornákon keresztül

A helyadatok MQTT protokollon keresztüli rejtett továbbítása, például gyorsulási vagy hőmérsékleti adatnak álcázva, szintén egy lehetséges megoldás a titkos adatgyűjtésre. Az MQTT protokoll, amelyet rugalmassága és sokoldalúsága miatt ismerünk, nem szab szigorú korlátozásokat a továbbított üzenetek jellegére vonatkozóan. Azonban egy ilyen rejtett adattovábbítás jelentős tervezést igényel. A legújabb kutatások [121] kimutatták, hogy egy személy két, különböző időpontban meghatározott helyzetének azonosítása lehetővé teszi, hogy következtessünk a személy kilétére, különösen speciális munkakörök esetében (a példában két CIA ügynök szerepel). Egy okosjármű és tulajdonosa fizikai helyzetének ismerete hasonló következményekkel járhat, mint az okostelefonok GPS-adatainak nyomon követése alkalmazásokon keresztül.

Egy személy fizikai helyzete a Föld felszínén koordinátákkal fejezhető ki, amely jellemzően szélességi és hosszúsági értékeket tartalmaz. Ezek a koordináták olyan adatokat jelentenek, amelyek meghatároznak egy konkrét pontot a Föld felszínén. A hely pontos kifejezésének precizitása több tényezőtől függ, beleértve a koordinátákban alkalmazott tizedesjegyek számát is.

A helyadatok rejtett csatornákon keresztüli továbbításának kihívása abban rejlik, hogy a geolokációs adatokat az üzenet hasznos adattartalmában úgy kell ábrázolni, hogy az elfedje az adattovábbítás valódi természetét, és más adatnak tűnjön. Ez magában foglalhatja a szélességi és hosszúsági koordináták numerikus értékként való kódolását,

vagy olyan kódolási sémák alkalmazását, amelyek a gyorsulásmérő értékeinek jellemzőit szimulálják. A rejtett továbbítás lényege az, hogy a geolokációs adatokat észrevétlenné tegye az üzenet tartalmában.

A szélességi és hosszúsági koordinátákat jellemzően fokokban fejezik ki, további tizedesjegyekkel a pontosság növelése érdekében. Egy koordináta tizedes részei fokperceket és fokmásodperceket is tartalmazhatnak a finomabb pontosság érdekében. A koordinátákban szereplő tizedesjegyek száma határozza meg a helymeghatározás pontossági szintjét. Például:

- Egy tizedesjeggyel rendelkező koordináta (pl. 40,1° N, 75,2° W) durva helymeghatározást ad, amely körülbelül 11 kilométeres pontosságú.
- Két tizedesjeggyel rendelkező koordináták (pl. 40,12° N, 75,24° W) körülbelül 1,1 kilométerre pontosítják a helyet.
- Három tizedesjegy (pl. 40,123° N, 75,246° W) körülbelül 110 méteres pontosságot biztosít.
- Négy tizedesjegy (pl. 40,1234° N, 75,2468° W) még nagyobb pontosságot kínál, körülbelül 11 méteres pontossággal.

A helyzet magas pontosságú kifejezése érdekében a koordináta további tizedesjegyeket is tartalmazhat, azonban gyakorlati szempontokat is figyelembe kell venni, mivel a túl sok tizedesjegy számítási bonyodalmakat okozhat, és a legtöbb alkalmazásban nem szükséges.

Az MQTT üzenetek hasznosadatainak manipulálása ideális alapot kínál a rejtett geolokációs adatok továbbítására, mivel numerikusan könnyen írható információ és emiatt nincs szükség fejlett szteganográfiai módszerek alkalmazására. A kulcs abban rejlik, hogy biztosítsuk, hogy az adatok egy megfigyelő számára tipikus formában, például gyorsulásmérő adatként jelenjenek meg.

6.4 A modellezési kísérlet eredményei

Kutatásom során három különböző adattípus (képek, hangfelvételek és helyadatok) rejtett továbbítását vizsgáltam az MQTT protokoll használatával.

A modelleim alkalmazása során azt feltételeztem, hogy az internetkapcsolattal rendelkező jármű valamely főbb szoftvereleme kompromittálódott, így bármely telematikai adat

vagy járműalkalmazásból származó információ hozzáférhető a támadó számára. Kutatásom az internetkapcsolattal rendelkező autó kommunikációjában létrejövő rejtett csatornákra összpontosított, különös tekintettel a rejtett csatorna lehetséges sávszélességére, amelyet a jármű különböző kommunikációs típusainak elemzésével vizsgáltunk. Feltételeztük, hogy az adattovábbítás sebességét csak a funkcionalitás korlátozza, a hálózati átviteli képességet (feltételezve gyors, 5G-hálózathoz kapcsolódó autókat) pedig nem vettük figyelembe a számítások során.

A képek és hangfelvételek esetében a szokásos adatcserével, ahol rejtett képeket és hangmintákat közvetlenül a telematikai adatok hasznosadatfolyamába ágyazunk, nem bizonyult hatékony megközelítésnek. Ez a korlát elsősorban azzal magyarázható, hogy ezen médiaformátumok egyszerűsített numerikus reprezentációkká történő átalakítása jelentős adatforgalmat igényel. Az ilyen nagy mennyiségű adat valós körülmények közötti továbbítása ésszerűtlenül hosszú időt igényelne.

Ezzel szemben az olyan fejlettebb funkciók, mint a fejlett autókövetés vagy az önvezető rendszerek elegendő sávszélességet biztosíthatnak ahhoz, hogy a támadók rejtett csatornákon keresztül akár ilyen mennyiségű adatokat is továbbítsanak.

A geolokációs adat minden adattovábbítási típushoz képest nagyobb alkalmazhatósági lehetőségeket mutatott a szteganográfiai technikákra vonatkozóan. A GPS adatok jól kódolhatók rejtett továbbításra, mivel a szokásos adatfajtáktól, például a gyorsulásmérő szenzoroktól származó adatoktól gyakorlatilag megkülönböztethetetlenné válik, köszönhetően a finom obfuszkációs mechanizmusoknak.

Eredményeinkből egyértelműen látszik, hogy a járművek egyre nagyobb mennyiségű adatot képesek továbbítani telekommunikációs hálózatokon keresztül, részben az olyan technológiai fejlesztéseknek köszönhetően, mint az 5G. Fontos megjegyezni, hogy a jelenleg lassúnak tűnő adattovábbítási technikák a jövőben jelentősen hatékonyabbá válhatnak. Ennek oka az adatátvitel költséghatékonyságának és egyszerűségének folyamatos növekedése, valamint a továbbítás gyorsaságának és könnyedségének növekedése. Ennek következtében az ebben a tanulmányban leírt időkeretek jelentősen rövidülhetnek, ami egyre inkább érdemessé teheti ezeknek a csatornáknak a kihasználását.

Tanulmányom során megfigyeléseket tettem és következtetéseket vontam le a személygépjárművek biztonságáról az adattovábbítási képességeik tekintetében.

Kutatásom rámutatott arra, hogy a személygépjárművek által továbbított adatok típusairól és mennyiségéről napjainkban nincs átfogó tanulmány. Vizsgálatom feltárta továbbá, hogy az olyan protokollok, mint az MQTT, rejtett csatornaként szolgálhatnak bizalmas információk továbbítására. Bár az MQTT önmagában nem ideális a nagy adatmennyiségek rejtett továbbítására, hatékonyan alkalmazható egyszerűbb adatfajták elrejtésére megfelelő szteganográfiai eszközökkel. Ezen megállapítások fényében javasolt e terület további kutatása.

Az autóiparban alkalmazott informatikai rendszerek átláthatóságának javítása kulcsszerepet játszhat a biztonság fokozásában, mivel elősegítheti a sebezhetőségek korai felismerését. Összegzésképpen, jelenlegi ismereteim alapján elképzelhető, hogy a járművekből adatok rejtett módon továbbíthatók a jármű tulajdonosának vagy akár a gyártó tudta nélkül. Ez rávilágít a folyamatos kutatás és éberség fontosságára az autóiparban megjelenő új biztonsági kihívások kezelésében. A fejezet eredményei alátámasztják a H2 hipotézist, rávilágítva arra, hogy a modern személygépjárművek komplex telematikai rendszerei és a kapcsolódó kommunikációs protokollok, mint az MQTT, valóban kockázatot hordoznak magukban, illetve olyan gyengeségekkel rendelkeznek, amelyeket rosszindulatú szereplők potenciálisan kihasználhatnak jogosulatlan adatátvitelre. Az elemzések megerősítették, hogy az autók, mint hálózatba kapcsolt eszközök, a rejtett csatornákon keresztül érzékeny információkat is továbbíthatnak, kihasználva a telematikai adatokba ágyazott üzeneteket. Az eredmények hangsúlyozzák a szabályozási keretek szigorításának szükségességét, hogy az adatbiztonsági kockázatok csökkenthetők legyenek, és az autók egyértelmű biztonsági irányelvek mentén működhessenek a digitális kommunikáció során.

ÖSSZEGZETT KÖVETKEZTETÉSEK

Megvizsgáltam a jelenlegi információbiztonsági környezetet a személygépjárművekre és a gyártókra vonatkozóan, és megállapítottam, hogy a jelenlegi szabályozások nem elégségesek az úgynevezett okosautók adatcseréjének megfelelő kontrollálásához, illetve az alapvető adatbiztonsági igények kielégítéséhez.

a. A jelenlegi szabályozás nem kezeli a személygépjárművet egységes informatikai eszközként, amely alapfeltétele lenne a megfelelő kontrollnak.

b. A jelenlegi szabályozás nem ír elő kötelező feltételeket az adatok küldésének szabványos módjával kapcsolatban.

c. A jelenlegi szabályozás nem teszi kötelezővé az adatcsere módjainak publikussá tételét semmilyen szinten.

Kérdőíves kutatást készítettem, melyben 289 személyt kérdeztem meg az okosautókkal kapcsolatos tapasztalatairól. A kérdőívet magyar és egyéb országokból származó személyek is kitöltötték.

a. A válaszadók jelentős része nem rendelkezett megfelelő információkkal arról, hogy járművük adatokat továbbít, illetve milyen típusú adatokat oszt meg a gyártóval és más harmadik felekkel. Az adatok alapján megállapítottam, hogy az átlagfelhasználók jelentős része nincs tisztában az okosautók adatkezelési gyakorlatával.

b. A válaszadók jelentős része úgy vélte, hogy fontos lenne, hogy a gyártók és szolgáltatók átlátható módon tájékoztassák a felhasználókat a jármű által továbbított adatokról és az adattovábbítás céljáról, azonban a tényleges tájékozottságuk ennek ellenére alacsony volt.

Mélyinterjút készítettem 10 magyarországi kiemelt szakértővel, amellyel a személygépjárművek adatküldésének információbiztonsági szintjét vizsgáltam. Megállapítottam, hogy nincs elfogadott gyakorlat vagy megosztott tudás a követendő irányelvekkel kapcsolatban.

a. A szakértők többsége úgy vélte, hogy az adatbiztonsági intézkedések nem tartanak lépést a technológia fejlődésével, és hogy hiányzik egy olyan központi szabályozó hatóság, amely az adatkezelési gyakorlatok betartását ellenőrizné.

b. Továbbá a szakértők arra is felhívták a figyelmet, hogy az információbiztonsági követelmények inkább az iparági szereplők önkéntes megfelelésére építenek, semmint kötelező szabályozási keretekre, amely akadályozza a megfelelő adatbiztonsági szint elérését a gyakorlatban.

c. Több szakértő felhívta a figyelmet arra, hogy egy szigorúbb és minden szereplőre kiterjedő kockázatkezelési keretrendszer javíthatja a tudatosságot és az adatbiztonságra vonatkozó követelményeknek való megfelelést.

Megvizsgáltam a rejtett adatküldés mennyiségének gyakorlati vonatkozásait, feltételezve, hogy a személygépjármű vagy annak valamely egysége kompromittált. Arra jutottam, hogy számos szolgáltatás képes lehet megfelelő mennyiségű rejtett adatot továbbítani, ami adatbiztonsági kockázatként jelentkezik a személyautók működése során.

a. Megállapítottam, hogy az okos járművek alapvető szenzorai képesek lehetnek havonta egy-két fénykép (utcakép) illetve néhány perces hangfelvételek elküldésére. Az állításomat számításokkal igazoltam.

b. Megállapítottam, hogy az okos járművek kényelmi funkciói (pl. önvezető modul) jelentős mennyiségű rejtett adat küldésére lehet alkalmas (pl. napi több utcakép). Az állításomat számításokkal igazoltam.

A személygépjármű, mint komplex informatikai termék a dolgozat eredményei alapján akkor érheti el a megfelelő információbiztonsági, kiberbiztonsági szintet, ha teljesülnek az olyan feltételek, mint például az adattovábbítási rendszer átláthatósága, a felhasználók megfelelő tájékoztatása, az adatok titkosított csatornán való küldése és a felhasználás kereteinek megszigorítása. Mivel ezt csak több szereplő együttes felügyeletével lehet elérni, így a megoldás egy olyan egységes kockázatmenedzsment rendszer bevezetése lehet, mely egyszerre érint minden szereplőt, növeli a szereplők biztonságtudatosságát, a veszélyek és fenyegetettségek átláthatóságát és melyet egy felügyelő hatóság ellenőrzni képes.

Új tudományos eredmények / Ajánlások

A vizsgálat során felmerült hipotézisek közül mindegyik alátámasztotta, hogy a jelenlegi jogi és szabályozási környezet nem képes teljes körű védelmet biztosítani az összetett informatikai rendszerekkel rendelkező modern gépjárművek esetében. A hipotézisek vizsgálata részletesen rávilágított arra, hogy a személygépjárművek információbiztonsági szempontból egyre közelebb állnak a Dolgok Internetéhez (IoT), és mint ilyenek, kiemelt célpontokká válhatnak a kiberbűnözés és a jogosulatlan adatgyűjtés szempontjából.

Az eredmények azt mutatják, hogy a jelenlegi információbiztonsági szabályozások főként a gyártókat vagy az egyes alrendszereket érintik, és kevésbé kezelik a járművet egységes informatikai rendszerként. A kutatás rámutatott arra, hogy az okosautók rendszerei, amelyek a biztonság, a navigáció és a szórakoztatás céljából széles körben használnak adatokat, könnyen sebezhetőek, és potenciálisan képesek rejtett adatküldésre a felhasználó tudta nélkül. Az eredmények szerint a tulajdonosok általában nincsenek tisztában a járművük által végzett adatátviteli folyamatokkal, és nem kapnak megfelelő tájékoztatást ezekről az adatküldési gyakorlatokról, ami jelentős kockázatokat hordoz az adatvédelem és a személyes adatok biztonsága szempontjából. Az eredmények megerősítették, hogy a személygépjárművek biztonságos informatikai eszközként való

kezeléséhez elengedhetetlen a titkosított adatforgalom, az átlátható adatáramlási folyamatok és egy felügyeleti hatóság kijelölése.

E kutatás jelentősége abban rejlik, hogy az adatalapú megfigyelés, a jármű-infrastruktúra közötti kommunikáció és az adatelemzés elterjedése egyaránt új adatvédelmi és adatbiztonsági kérdéseket és biztonsági kockázatokat vet fel. Az okosjárművek adatbiztonsági kihívásainak értékelésével a dolgozat új megvilágításba helyezi az autóipari információbiztonsági követelményeket, és hangsúlyozza az átfogó megközelítés fontosságát. A kutatás eredményei kiemelik, hogy a járművek digitális ökoszisztémájának adatvédelmi és biztonsági kihívásai új szabályozási intézkedéseket, átfogó kockázatkezelési keretrendszereket, valamint az adatbiztonsági szabványok hatékonyabb alkalmazását teszik szükségessé.

Az eredmények fényében fontos, hogy a jövőbeli kutatások az autók, mint kiberfizikai rendszerek, átfogó biztonsági kérdéseire koncentráljanak. További kutatások szükségesek annak megértéséhez, hogy miként lehet az IoT eszközökre vonatkozó szabványokat a járművek esetében alkalmazni és fordítva, hogyan hangolhatóak ezek össze, és milyen új szabályozások támogathatják a járművek védelmét, különösen a hálózati kapcsolódás, a távoli frissítések és a valós idejű adatfeldolgozás terén. Jövőbeli kutatási irány lehet a titkosított adatforgalom és a rejtett csatornák járműspecifikus elemzése. Ez az elemzésen túl magában foglalhatja új algoritmusok, titkosítási módszerek és hálózati protokollok kidolgozását, amelyek segíthetik a rejtett adatcsatornák felismerését és megakadályozását.

A jelenlegi szabványok és jogszabályok tekintetében meg kell vizsgálni, milyen módosítások eszközölhetőek, amelyek segítenek a megfelelő kockázatkezelési módszertan kifejlesztésében és elterjesztésében a feltárt hiányosságok csökkentésével. Érdemes megvizsgálni, hogy milyen akadályai vannak egy Európai Uniós szintű vagy helyi hatóság, illetve hatóságok felállításának, amelyek megkövetelik és betartatják a követelményeket. Szintén érdekes kutatási irány lehet annak vizsgálata, hogy mi tehetné vonzóbbá a szabványok elterjesztését és betartatását kezdve a lehetséges veszélyek tudatosításától az auditdíjak és büntetések arányának vizsgálatáig.

Ezen túlmenően a felhasználói tudatosság növelésére irányuló kutatások szintén kulcsfontosságúak, hiszen a fogyasztók információbiztonsági tudatosságának hiánya könnyű célponttá teszi őket. Olyan edukációs programok kidolgozása, amelyek lehetővé

teszik a felhasználók számára, hogy megértsék az adataik biztonságának fontosságát, hozzájárulhat a személygépjármű-ipari információbiztonsági szabványok betartásához és a gyártók iránti bizalom fenntartásához.

IRODALOMJEGYZÉK

[1] Hofmann, Martin; Neukart, Florian; Bäck, Thomas: Artificial Intelligence and Data Science in the Automotive Industry, 2017.

[2] Marabelli, M.; Hansen, S.; Newell, S.; Frigerio, C.: The Light and Dark Side of the Black Box: Sensor-based Technology in the Automotive Industry. *Communications of the Association for Information Systems*, 40(16) (2017), pp. 368–388.

[3] Ogbuke, Nnamdi Johnson; Yusuf, Yahaya Y.; Dharma, Kovvuri; Mercangoz, Burcu A.: Big data supply chain analytics: ethical, privacy and security challenges posed to business, industries and society. *Production Planning & Control*, 31(11–12) (2020), pp. 965–978.

[4] Ivanov, Dimitry; Dolgui, Alexandre: A Digital Supply Chain Twin for Managing the Disruption Risks and Resilience in the Era of Industry 4.0. *Production Planning & Control*, 31(11–12) (2020), pp. 935–948.

[5] Modernizáció és iparbiztonság a COVID-19-járvány után. In: BABOS, Tibor (szerk.): Digitális Biztonságpolitika a Kibertérben: Tanulmánykötet. Gödöllő, Magyarország: Magyar Agrár- és Élettudományi Egyetem, 2021. pp. 101-131.

[6] Oliver, N.; Pentland, A. P.: Driver Behavior Recognition and Prediction in a SmartCar, 2000.

[7] Peppes, Nikolaos; Alexakis, Theodoros; Adamopoulou, Evgenia; Demestichas, Konstantinos: Driver Behavior Monitoring Based on Smartphone Sensor Data and Machine Learning Methods. In *2019 25th Conference of Open Innovations Association (FRUCT)* (2019), pp. 1–7.

[8] Juhász László: A Karbantartás 4.0 helyzetének elemzése a hazai járműiparban. Óbudai Egyetem, Elérhető: http://www.lib.uni-obuda.hu/sites/lib.uni-obuda.hu/files/Juhasz_Laszlo_ertekezes.pdf (Letöltve: 2024.11.17.)

[9] McKinsey & Company: Car connectivity: What consumers want and are willing to pay. Elérhető: https://www.mckinsey.com/industries/automotive-and-assembly/our-insights/car-connectivity-what-consumers-want-and-are-willing-to-pay (Letöltve: 2024.11.17.)

[10] Airlinq: 8 Industries Being Transformed by Connected Car Data. Elérhető: https://www.airlinq.com/8-industries-being-transformed-by-connected-car-data/ (Letöltve: 2024.11.17.)

[11] MDPI Sensors: Sensors: Special Issue on Advanced Connected Vehicle Technology. 21(22), 2021. Elérhető: https://www.mdpi.com/1424-8220/21/22/7712 (Letöltve: 2024.11.17.)

[12] IEEE: Connected Vehicle Security Threat Analysis. IEEE Access, 2018. Elérhető: https://ieeexplore.ieee.org/document/8515151 (Letöltve: 2024.11.17.)

[13] Pinsent Masons: The connected car raises a new world of data management, privacy, and ownership. Elérhető: https://www.pinsentmasons.com/out-law/analysis/the-connected-car-raises-new-world-of-data-management-privacy-and-ownership (Letöltve: 2024.11.17.)

[14] McKinsey & Company: Car connectivity: What consumers want and are willing to pay. Elérhető: https://www.mckinsey.com/industries/automotive-and-assembly/our-insights/car-connectivity-what-consumers-want-and-are-willing-to-pay (Letöltve: 2024.11.17.)

[15] Airlinq: 8 Industries Being Transformed by Connected Car Data. Elérhető: https://www.airlinq.com/8-industries-being-transformed-by-connected-car-data/ (Letöltve: 2024.11.17.)

[16] Pinsent Masons: The connected car raises a new world of data management, privacy, and ownership. Elérhető: https://www.pinsentmasons.com/out-law/analysis/the-connected-car-raises-new-world-of-data-management-privacy-and-ownership (Letöltve: 2024.11.17.)

[17] Dombora Sándor: Eredményes információbiztonsági rendszerek kialakítása és bevezetése. Óbudai Egyetem. Elérhető: http://www.lib.uni-obuda.hu/sites/lib.uni-obuda.hu/files/Dombora_Sandor_ertekezes.pdf (Letöltve: 2024.11.17.)

[18] Wired: GM Took 5 Years to Fix a Full-Takeover Hack on Millions of OnStar Cars. Elérhető: https://www.wired.com/2015/09/gm-took-5-years-fix-full-takeover-hack-millions-onstar-cars/#:~:text=7%3A00%20AM-,GM%20Took%205%20Years%20to%20Fix%20a%20Full%2DTakeover%20Hack,known%20remote%20car%20hacking%20technique. (Letöltve: 2024.11.17.)

[19] Wired: Hackers Remotely Kill a Jeep on the Highway. Elérhető: https://www.wired.com/2015/07/hackers-remotely-kill-jeep-highway/ (Letöltve: 2024.11.17.)

[20] Sam Curry: Hacking Kia. Elérhető: https://samcurry.net/hacking-kia (Letöltve: 2024.11.17.)

[21] Al-Saadi, M., & Hammad, M.: Connected vehicles: Technology review, state of the art, challenges and opportunities. Sensors, 21(22) (2021), p. 7712. DOI: https://doi.org/10.3390/s21227712.

[22] U.S. Department of Transportation: How connected vehicles work. Elérhető: https://www.transportation.gov/research-and-technology/how-connected-vehicles-work (Letöltve: 2024.11.17.)

[23] Curry, S.: Web Hackers vs. The Auto Industry: Critical Vulnerabilities in Ferrari, BMW, Rolls Royce, Porsche, and More. Samcurry.net, 2023. Elérhető: https://samcurry.net/web-hackers-vs-the-auto-industry/ (Letöltve: 2024.11.17.)

[24] Koubatis, A., Schoenborn, J. T.: Risk management of complex critical systems. International Journal of Critical Infrastructures, 1(2/3) (2005), pp. 200–213. DOI: 10.1504/IJCIS.2005.007974. (Letöltve: 2024.11.17.)

[25] Gardner, D.: Risk: The Science and Politics of Fear. Random House, New York, 2009. ISBN: 978-0-307-35643-7. (Letöltve: 2024.11.17.)

[26] Ellerby, Z., McCulloch, J., Wilson, M., Wagner, C.: Exploring How Component Factors and Their Uncertainty Affect Judgements of Risk in Cyber-Security. In: Gritzalis, D., Theocharidou, M., Stergiopoulos, G. (eds) Critical Information Infrastructures Security. CRITIS 2019. Lecture Notes in Computer Science, vol 11777. Springer, Cham, 2020. pp. 35–47. DOI: 10.1007/978-3-030-37670-3_3.

[27] State Council: Decision on Accelerating the Cultivation and Development of Strategic Emerging Industries. Released in October 2010. Elérhető: http://www.gov.cn/zwgk/2010-10/18/content_1724848.htm (Letöltve: 2024.11.17.)

[28] Zhang, X., Liang, Y., Yu, E., Rao, R., Xie, J.: Review of electric vehicle policies in China: Content summary and effect analysis. Renewable and Sustainable Energy Reviews, 70 (2017), pp. 698–714. DOI: https://doi.org/10.1016/j.rser.2016.11.250.

[29] Wang, N., Tang, L., Pan, H.: A global comparison and assessment of incentive policy on electric vehicle promotion. Sustainable Cities and Society, 44 (2019), pp. 597–603. DOI: 10.1016/j.scs.2018.10.024.

[30] China Mobile: Source Environmental Management Annual Report 2020. Elérhető: https://www.chinamobileltd.com/en/ir/reports/ar2020/sd2020.pdf (Letöltve: 2024.11.17.)

[31] Guo, D., Yan, W., Gao, X., Hao, Y., Xu, Y., E, W., Zhang, T.: Forecast of passenger car market structure and environmental impact analysis in China. Science of The Total Environment, 772 (2021), p. 144950. DOI: 10.1016/j.scitotenv.2021.144950.

[32] Wang, N., Pan, H., Zheng, W.: Assessment of the incentives on electric vehicle promotion in China. Transportation Research Part A: Policy and Practice, 101 (2017), pp. 177–189. DOI: 10.1016/j.tra.2017.05.016.

[33] Ibold, S., Xia, Y., Xiao, S.: NEV Development Plan 2035 - Policy Briefing & English Translation. Deutsche Gesellschaft für Internationale Zusammenarbeit (GIZ) GmbH, Beijing, 2021. Elérhető: https://www.mobility.transition-china.org/ (Letöltve: 2024.11.17.)

[34] Xu, L., & Su, J.: From government to market and from producer to consumer: Transition of policy mix towards clean mobility in China. Energy Policy, 96 (2016), pp. 328–340. DOI: 10.1016/j.enpol.2016.06.017. (Letöltve: 2024.11.17.)

[35] Ji, Z., Huang, X.: Plug-in electric vehicle charging infrastructure deployment of China towards 2020: Policies, methodologies, and challenges. Renewable and Sustainable Energy Reviews, 90 (2018), pp. 710–727. DOI: 10.1016/j.rser.2018.03.048. (Letöltve: 2024.11.17.)

[36] Andersen, P. H., Mathews, J. A., Rask, M.: Integrating private transport into renewable energy policy: The strategy of creating intelligent recharging grids for electric vehicles. Energy Policy, 37(7) (2009), pp. 2481–2486. DOI: 10.1016/j.enpol.2009.03.032. (Letöltve: 2024.11.17.)

[37] Mitra, S.: China's innovation advantage. Forbes, 2009. Elérhető: http://www.forbes.com/2009/08/06/china-innovation-dcm-intelligent-technology-david-chao.html (Letöltve: 2024.08.12.)

[38] Charitou, C. D., Markides, C. C.: Responses to disruptive strategic innovation. MIT Sloan Management Review, 44 (2003), pp. 55–63.

[39] Thukral, I. S., Von Ehr, J., Walsh, S., Groen, A. J., Van Der Sijde, P., Akmaliah Adham, K.: Entrepreneurship, emerging technologies, emerging markets. International Small Business Journal, 26(1) (2008), pp. 101–116. DOI: 10.1177/0266242607084659.

[40] Li, W., Long, R., Chen, H.: Consumers' evaluation of national new energy vehicle policy in China: an analysis based on a four paradigm model. Energy Policy, 99 (2016), pp. 33–41. DOI: 10.1016/j.enpol.2016.09.001.

[41] Krug, B.: Ties that Bind: The Emergence of Entrepreneurs in China. ERS-2000-44-ORG, Erasmus Research Institute of Management, Rotterdam, 2000.

[42] Krug, B., Hendrischke, H.: Framing China: Transformation and institutional change through co-evolution. Management and Organization Review, 4(1) (2008), pp. 81–108.

[43] Krug, B., Polos, L.: The Strawberry Growth Underneath the Nettle: The Emergence of Entrepreneurs in China. ERS-2000-34-ORG, Erasmus Research Institute of Management, Rotterdam, 2000.

[44] Jin, B., Li, J.: Ownership structure and new product development in transitional economies: An empirical study in China. International Journal of Production Economics, 107(2) (2007), pp. 422–439. DOI: 10.1016/j.ijpe.2006.08.010.

[45] Wang, H., Kimble, C.: Betting on Chinese electric cars? – Analysing BYD's capacity for innovation. International Journal of Automotive Technology and Management, 10(1) (2010), p. 77. DOI: 10.1504/IJATM.2010.031457.

[46] Beaume, R., Midler, C.: From technology competition to reinventing individual ecomobility: New design strategies for electric vehicles. International Journal of Automotive Technology and Management, 9(2) (2009), pp. 174–190. DOI: 10.1504/IJATM.2009.023939.

[47] Wang, H., Kimble, C.: Betting on Chinese electric cars? – Analysing BYD's capacity for innovation. International Journal of Automotive Technology and Management, 10(1) (2010), p. 77. DOI: 10.1504/IJATM.2010.031457.

[48] Wu, Y. A., Ng, A. W., Yu, Z., Huang, J., Meng, K., Dong, Z. Y.: A review of evolutionary policy incentives for sustainable development of electric vehicles in China: Strategic implications. Energy Policy, 148, Part B (2021), p. 111983. DOI: 10.1016/j.enpol.2020.111983.

[49] Yang, D., Meng, J., Yang, L., Nie, P., Wu, Q.: Dual-Credit Policy of new energy automobile at China: Inhibiting scale or intermediary of innovation? Energy Strategy Reviews, 43 (2022), p. 100932. DOI: 10.1016/j.esr.2022.100932.

[50] Zhou, Y., Wang, M., Hao, H., Johnson, L., Wang, H.: Plug-in electric vehicle market penetration and incentives: a global review. Mitigation and Adaptation Strategies for Global Change, 20 (2015), pp. 777–795. DOI: 10.1007/s11027-014-9611-2.

[51] Liu, Y., Zhao, X., Lu, D., Li, X.: Impact of policy incentives on the adoption of electric vehicles in China. Transportation Research Part A: Policy and Practice, 176 (2023), p. 103801. DOI: 10.1016/j.tra.2023.103801.

[52] Mock, P., Yang, Z.: Driving electrification: a global comparison of fiscal incentive policy for electric vehicles. Experimental Physiology, 98(98) (2013), pp. 1244–1246. DOI: 10.1113/expphysiol.2013.077826.

[53] Lieven, T.: Policy measures to promote electric mobility – a global perspective. Transportation Research Part A: Policy and Practice, 82 (2015), pp. 78–93. DOI: 10.1016/j.tra.2015.09.008.

[54] Zheng, J., Mehndiratta, S., Guo, J. Y., Liu, Z.: Strategic policies and demonstration program of electric vehicle in China. Transport Policy, 19(1) (2012), pp. 17–25. DOI: 10.1016/j.tranpol.2011.07.006.

[55] Hu, X., Chang, S., Li, J., Qin, Y.: Energy for sustainable road transportation in China: Challenges, initiatives and policy implications. Energy, 35(11) (2010), pp. 4289–4301. DOI: 10.1016/j.energy.2009.05.024.

[56] Ou, S., Lin, Z., He, X., Yu, R., Bouchard, J., Przesmitzki, S.: Forecasting the Impact of Dual-credit Policy (2021–2023) on China's Electric Vehicle Market. 33rd World Electric Vehicle

Symposium & Exposition (EVS33), Portland, Oregon, June 14–17, 2020. Elérhető: https://www.evs33.org/ (Letöltve: 2024.11.17.)

[57 Y1] Statista. (2023). Annual sales of new energy vehicles in China 2011-2023, by propulsion type. Elérhető: https://www.statista.com/statistics/425466/china-annual-new-energy-vehicle-sales-by-type

[58] European Environment Agency (EEA): New registrations of electric vehicles. Elérhető: https://www.eea.europa.eu/ims/new-registrations-of-electric-vehicles (Letöltve: 2024.11.17.)

[59] European Automobile Manufacturers' Association (ACEA): The Automobile Industry Pocket Guide 2021/2022. (2020) Elérhető: https://www.acea.auto/files/ACEA_Pocket_Guide_2021-2022.pdf (Letöltve: 2024.11.17.)

[60] Rutishauser, P.: Chinese auto brands coming to Europe: full report. sophus3, 2022. Elérhető: https://www.sophus3.com/sophus3-briefing-paper-chinese-auto-brands-in-europe-part-1/ (Letöltve: 2024.11.17.)

[61] European Automobile Manufacturers' Association (ACEA): Economic and Market Report: State of the EU auto industry - First three quarters of 2021. November 2021. Elérhető: https://www.acea.auto/files/Economic_and_Market_Report-First_three_quarters_of_2021.pdf (Letöltve: 2024.11.17.)

[62] MERICS: China Monitor: The Automotive Industry. 2021. Elérhető: https://merics.org/sites/default/files/2021-09/MericsChinaMonitorAutomotiveindustry%2071_final2_1.pdf (Letöltve: 2024.11.17.)

[63] MERICS: Made in China: Electric vehicles could turn Sino-EU trade on its head. 2022. Elérhető: https://merics.org/en/short-analysis/made-china-electric-vehicles-could-turn-sino-eu-trade-its-head (Letöltve: 2024.11.17.)

[64] Schmidt, M.: Is China's Electric Car Tiger About to Bite? 2022. Elérhető: https://www.schmidtmatthias.de/post/is-china-s-electric-car-tiger-about-to-bite (Letöltve: 2024.11.17.)

[65] Horváth, Zsolt: TISAX, az autóipar új információbiztonsági követelményrendszere. Magyar Minőség, június (2020). Elérhető: https://infobiz.hu/images/Publikaciok/Magyar_Minsg_2020_06_cikk_HZs_TISAX.pdf. (Letöltve: 2024.11.17.)

[66] Dominique Machuletz, Rainer Böhme: Multiple Purposes, Multiple Problems: A User Study of Consent Dialogs after GDPR. Proceedings on Privacy Enhancing Technologies, 2020(2) (2020), pp. 481–498. DOI: 10.2478/popets-2020-0037.

[67] Laura A. Stoica, Radu A. C. Savu: Risks and Exploits Exposed by GDPR. Eurasian Journal of Social Sciences, 9(1) (2021), pp. 1–8. DOI: 10.15604/ejss.2021.09.01.001.

[68] Alexander Gladis, Nils J. Hartwich, Oliver Salge: Weaponizing the GDPR: How Flawed Implementations Turn the Gold Standard for Privacy Laws into Fool's Gold. In: Proceedings of the 43rd International Conference on Information Systems (ICIS 2022), Koppenhága, 2022. Elérhető: https://aisel.aisnet.org/icis2022/proceedings/Privacy/3/. (Letöltve: 2024.11.17.)

[69] United Nations Economic Commission for Europe (UNECE): Three landmark UN vehicle regulations enter into force. 2021. Elérhető: https://unece.org/sustainable-development/press/three-landmark-un-vehicle-regulations-enter-force (Letöltve: 2024.11.17.)

[69] Marcinek, M. (2020). Cybercrime in Automotive Security in the 21th Century. *Internal Security*, *12*(2), 191–200. https://doi.org/10.5604/01.3001.0014.6694

[70] Braun, V., Clarke, V.: Using thematic analysis in psychology. Qualitative Research in Psychology, 3(2) (2006), pp. 77–101. Elérhető: https://dl1.cuni.cz/pluginfile.php/1195620/mod_folder/content/0/Braun%20and%20Clarke%202006%20Thematic%20analysis.pdf (Letöltve: 2024.11.17.)

[71] Schmittner, C., Ma, Z., Reyes, C., Dillinger, O., Puschner, P.: Using SAE J3061 for Automotive Security Requirement Engineering. In: Skavhaug, A., Guiochet, J., Schoitsch, E., Bitsch, F. (eds) Computer Safety, Reliability, and Security. SAFECOMP 2016. Lecture Notes in Computer Science, vol 9923. Springer, Cham, 2016. DOI: 10.1007/978-3-319-45480-1_13.

[72] Fowler, F. J., Couper, M. P., Lepkowski, J. M.: Survey Methodology. John Wiley & Sons, 2011. ISBN: 978-0470465462.

[73] Gideon, L.: Handbook of Survey Methodology for the Social Sciences. Springer, 2012. DOI: 10.1007/978-1-4614-3876-2.

[74] Bairagi, V., Munot, M. V.: Research Methodology: A Practical and Scientific Approach. CRC Press, 2019. ISBN: 978-0367256206.

[75] Adams, J., Khan, H. T. A., Raeside, R., White, D.: Research Methods for Graduate Business and Social Science Students. SAGE Publications, 2007. ISBN: 978-0761935896.

[76] Creswell, J. W., Plano Clark, V. L.: Designing and Conducting Mixed Methods Research. 2. kiadás. Sage Publications, 2011. Elérhető: https://archive.org/details/designingconduct0000cres_i7e7 (Letöltve: 2024.11.17.)

[77] Guttman, L.: A basis for analyzing test-retest reliability. Psychometrika, 10(4) (1945), pp. 255–282. Elérhető: https://www.scirp.org/reference/referencespapers?referenceid=2984730 (Letöltve: 2024.11.17.)

[78] McNeish, D.: Thanks coefficient alpha, we'll take it from here: Moving beyond “reliability” to greater specificity, flexibility, and transparency. Psychological Methods, 23(3) (2018), pp. 412–433. DOI: 10.1037/met0000144. Elérhető: https://journals.sagepub.com/doi/full/10.1177/2515245920951747 (Letöltve: 2024.11.17.)

[79] Sijtsma, K.: On the use, the misuse, and the very limited usefulness of Cronbach's alpha. Psychometrika, 74(1) (2009), pp. 107–120. DOI: 10.1007/s11336-008-9101-0. Elérhető: https://link.springer.com/article/10.1007/s11336-008-9101-0 (Letöltve: 2024.11.17.)

[80] Dombora, S.: Eredményes információbiztonsági rendszerek kialakítása és bevezetése. Doktori értekezés, 2022. Elérhető: https://doktori.hu/index.php?menuid=193&lang=HU&vid=25031 (Letöltve: 2024.11.17.)

[81] Khan, Shah Khalid; Shiwakoti, Nirajan; Stasinopoulos, Peter; Chen, Yilun: Cyber-attacks in the next-generation cars, mitigation techniques, anticipated readiness and future directions. *Accident Analysis & Prevention*, 148 (2020), p. 105837.

[82] Weimerskirch, A., Gaynier, R.: An Overview of Automotive Cybersecurity: Challenges and Solution Approaches, 2015.

[83] Koubatis, Andrew; Schonberger, Jorge Yerena: Risk management of complex critical systems. *International Journal of Critical Infrastructures*, 1(2/3) (2005), pp. 200–213.

[84] Gardner, D.: *Risk: The Science and Politics of Fear*. Random House, New York, 2009.

[85] Ellerby, Zack; McCulloch, Josie; Wilson, Melanie; Wagner, Christian: Exploring How Component Factors and Their Uncertainty Affect Judgements of Risk in Cyber-Security. *Critical Information Infrastructures Security. Lecture Notes in Computer Science*, 11777 (2020), pp. 15–26.

[86] Ji, Zuzhen; Yang, Shuang-Hua; Cao, Yi; Wang, Yuchen; Zhou, Chenchen; Yue, Liang; Zhang, Yinqiao: Harmonizing safety and security risk analysis and prevention in cyber-physical systems. *Process Safety and Environmental Protection*, 148 (2021), pp. 1–10.

[87] Mouha, R.: Internet of Things (IoT). *Journal of Data Analysis and Information Processing*, 9 (2021), pp. 1–12.

[88] Szczepaniuk, H.; Szczepaniuk, E. K.: Standardization of IoT Ecosystems: Open Challenges, Current Solutions, and Future Directions. CRC Press, 2022.

[89] Kelemen-Erdős, Anikó; Mitev, Ariel: Holisztikus szolgáltatásélmény-vendég-utazás és kölcsönös értékteremtés dimenziói az art-és romkocsmák példáján. *Marketing & Menedzsment*, 50(3–4) (2016), pp. 45–56.

[90] Babbie, Earl: A társadalomtudományi kutatás gyakorlata. Balassi Kiadó, 2020.

[91] Kelemen-Erdős, Anikó; Mitev, Ariel: Tematikus szolgáltatásélmény art-és romkocsma környezetben. *Turisztikai és Vidékfejlesztési Tanulmányok*, 2(3) (2017), pp. 45–56.

[92] Kelemen-Erdős, Anikó; Molnár, Adél: Cooperation or conflict? The nature of the collaboration of Marketing and Sales organizational units. *Economics and Culture*, 16(1) (2019), pp. 45–56.

[93] Krippendorff, K.: *Content Analysis. An Introduction to Its Methodology*. Thousand Oaks: SAGE, 2018.

[94] Stecklow, S., Cunningham, W., & Jin, H. (2023, április 6.). Special Report: Tesla workers shared sensitive images recorded by customer cars. Reuters. Elérhető itt: https://www.reuters.com/article/tesla-privacy-cameras-idCAKBN2W310G

[95] Dorri, A., Steger, M., Kanhere, S. S., & Jurdak, R. (2019). A blockchain-based solution to automotive security and privacy. In Blockchain for Distributed Systems Security (pp. 95-116).

[96] N. Hussein and A. Nhlabatsi, "Living in the Dark: MQTT-Based Exploitation of IoT Security Vulnerabilities in ZigBee Networks for Smart Lighting Control," IoT, vol. 3, no. 4, pp. 450-472, Nov. 2022, doi: 10.3390/iot3040024.

[97] M. Praveen, A. Raza, és M. Hasib, "Open-Source Security Testing Tools for IoT Protocols - MQTT and Zigbee," IEEE, PDF. doi: 10.1109/ASET56582.2023.10180709

[98] I. Vaccari, S. Narteni, M. Aiello, M. Mongelli and E. Cambiaso, "Exploiting Internet of Things Protocols for Malicious Data Exfiltration Activities," in IEEE Access, vol. 9, pp. 104261-104280, 2021, doi: 10.1109/ACCESS.2021.3099642

[99] A. J. Hintaw, S. Manickam, M. F. Aboalmaaly, és S. Karuppayah, "MQTT Vulnerabilities, Attack Vectors and Solutions in the Internet of Things (IoT)," IETE Journal of Research, vol. 69, no. 6, pp. 3368-3397, May 4, 2021. doi: 10.1080/03772063.2021.1912651

[100] A. Koubatis és J. Schonberger, "Risk management of complex critical systems," IJCIS, kötet 1, oldalak 195-215, 2005. doi: 10.1504/IJCIS.2005.006119.

[101] H. Hegyi, "The Information Security of Personal Vehicles from the Perspective of Information Security Experts," JOURNAL OF SECURITY SCIENCE, vol. 5, no. 2, pp. 47–58, 2023.

[102] A. J. Hintaw, S. Manickam, M. F. Aboalmaaly, és S. Karuppayah, "MQTT Vulnerabilities, Attack Vectors and Solutions in the Internet of Things (IoT)," IETE Journal of Research, vol. 69, no. 6, pp. 3368-3397, May 4, 2021.

[103] J. Bourne, "China's Tesla restrictions expose growing concern about AVs' digital privacy," Insider Intelligence, Jun. 23, 2022. [Online]. Available: https://www.insiderintelligence.com/content/china-s-tesla-restrictions-expose-growing-concern-about-avs-digital-privacy.

[104] Bergmann, Svenja; Seeliger, Arne; Cenedese, Alberto: Visualizing Time Series Data for Early Stage Business Analytics - The Case of Vehicle Telematics Data. 2022.

[105] Ullah, A.; Abdullah, A. H.; Amiri, I. S.; Said, M. B. H.: Connected Vehicles: Solutions and Challenges. IEEE Transactions on Vehicular Technology, vol. 67, no. 9 (2018), pp. 8346–8357. DOI: 10.1109/TVT.2018.2852850.

[106] Kumari, S.; Singh, A. K.; Reddy, A. V. R.; Kumari, S.: IoT-Connected Vehicle for Future Networks: A Review. IEEE Access, vol. 7 (2019), pp. 124857–124874. DOI: 10.1109/ACCESS.2019.2940000.

[107] HiveMQ: MQTT Standard for Connected Car. Elérhető: https://www.hivemq.com/article/mqtt-standard-for-connected-car/ (Letöltve: 2024.11.17.)

[108] Denning, D. E.: Secure personal computing in an insecure network. Communications of the ACM, vol. 22, no. 8 (1979), pp. 476–482. DOI: 10.1145/359138.359143.

[109] Dutta, A.; Hammad, E.: 5G Security Challenges and Opportunities: A System Approach. 2020 IEEE 3rd 5G World Forum (5GWF), Bangalore, India, 2020, pp. 109–114. DOI: 10.1109/5GWF49715.2020.9221122.

[110] Mileva, A.; Velinov, A.; Hartmann, L.; Wendzel, S., et al.: Comprehensive analysis of MQTT 5.0 susceptibility to network covert channels. Computers & Security, vol. 102 (2021). DOI: 10.1016/j.cose.2021.102027.

[111] Velinov, A.; Mileva, A.; Wendzel, S.; Mazurczyk, W.: Covert channels in the MQTT-based Internet of Things. IEEE Access (2019). Elérhető: https://ieeexplore.ieee.org/document/8890870 (Letöltve: 2024.11.17.)

[112] Caltrider, J.; Rykov, M.; MacDonald, Z.: What Data Does My Car Collect About Me and Where Does It Go? Mozilla Foundation, 2023. Elérhető: https://foundation.mozilla.org/en/privacynotincluded/articles/what-data-does-my-car-collect-about-me-and-where-does-it-go/ (Letöltve: 2024.11.17.)

[113] Hutchins, E. M., Cloppert, M. J., és Amin, R. M., "Intelligence-Driven Computer Network Defense Informed by Analysis of Adversary Campaigns and Intrusion Kill Chains," Lockheed Martin Corporation, 2011.

[114] KDnuggets: How to Convert a Picture into Numbers. Elérhető: https://www.kdnuggets.com/2020/01/convert-picture-numbers.html (Letöltve: 2024.11.17.)

[115] Fridrich, J.; Goljan, M.; Soukal, D.: Perturbed quantization steganography with wet paper codes. MM&Sec '04: Proceedings of the 2004 workshop on Multimedia and security, Sep. 2004, pp. 4–15. DOI: 10.1145/1022431.1022435.

[116] Almohammad, A.; Ghinea, G.; Hierons, R. M.: JPEG Steganography: A Performance Evaluation of Quantization Tables. 2009 International Conference on Advanced Information Networking and Applications, Bradford, UK, 2009, pp. 471–478. DOI: 10.1109/AINA.2009.67.

[117] Djebbar, F.; Ayad, B.; Meraim, K. Abed; Hamam, H.: Comparative study of digital audio steganography techniques. EURASIP Journal on Audio, Speech, and Music Processing, vol. 2012, no. 25 (2012).

[118] Iwakami, N.; Moriya, T.; Miki, S.: High-quality audio-coding at less than 64 kbit/s by using transform-domain weighted interleave vector quantization (TwinVQ). 1995 International Conference on Acoustics, Speech, and Signal Processing, Detroit, MI, USA, 1995, pp. 3095–3098. DOI: 10.1109/ICASSP.1995.479500.

[119] Tsung-Han, T.; Yen, C.-C.: A high quality re-quantization/quantization method for MP3 and MPEG-4 AAC audio coding. 2002 IEEE International Symposium on Circuits and Systems (ISCAS), Phoenix-Scottsdale, AZ, USA, 2002, pp. III–III. DOI: 10.1109/ISCAS.2002.1010358.

[120] FreeThink: Microsoft’s new AI needs just 3 seconds of audio to clone a voice. Elérhető: https://www.freethink.com/robots-ai/voice-cloning-vall-e (Letöltve: 2024.11.17.)

[121] The Intercept, “American phone-tracking firm demoed surveillance powers by spying on CIA and NSA”
URL:https://theintercept.com/2022/04/22/anomaly-six-phone-tracking-zignal-surveillance-cia-nsa/

TÁBLÁZATJEGYZÉK

ÁBRAJEGYZÉK

RÖVIDÍTÉSJEGYZÉK

Rövidítés	Jelentés (angol)	Magyar megfelelők
ACEA	European Automobile Manufacturers' Association	Európai Autógyártók Szövetsége
ADAS	Advanced Driver Assistance Systems	Fejlett vezetőtámogató rendszerek
API	Application Programming Interface	Alkalmazásprogramozási felület
ASPICE	Automotive Software Process Improvement and Capability dEtermination	Járműipari szoftverfolyamat-fejlesztés és képesség-meghatározás
AUTOSAR	AUTomotive Open System ARchitecture	Autóipari Nyílt Rendszer Architektúra
AVIF	AV1 Image File Format	AV1 Fájlformátum
BEV	Battery Electric Vehicle	Akkumulátoros elektromos jármű
BYD	Build Your Dreams	Build Your Dreams (márkanév)
CCTV	Closed-Circuit Television	Zárt rendszerű televízió (megfigyelőkamerarendszer)
CISPR	International Special Committee on Radio Interference	Nemzetközi Rádiózavartási Bizottság
CO2	Carbon Dioxide	Széndioxid
CoAP	Constrained Application Protocol	Korlátozott Alkalmazási Protokoll
COVID	COronaVIrus Disease	Koronavírus betegség
CR	Covert Receiver	Rejtett vevő
CS	Covert Sender	Rejtett küldő
CSMS	Cyber Security Management System	Kiberbiztonsági irányítási rendszer
DCC	Direct Covert Channel	Közvetlen rejtett csatorna
ECU	Electronic Controller Unit	Elektronikus vezérlőegység
ERGO	Electric Recharge Grid Operator	Elektromos töltőhálózat-üzemeltető
EV	Electric Vehicle	Elektromos jármű

FOTA	Firmware Over the Air	Szoftverfrissítés vezeték nélkül
GDPR	General Data Privacy Regulation	Általános adatvédelmi rendelet
GIF	Graphics Interchange Format	Graphics Interchange Format (formátum)
GM	General Motors	General Motors (autógyártó)
GPS	Global Positioning System	Globális helymeghatározó rendszer
HTTP	Hypertext Transfer Protocol	Hipertext átvitel protokoll
HTTPS	Hypertext Transfer Protocol Secure	Titkosított hipertext átvitel protokoll
ICC	Indirect Covert Channel	Közvetett rejtett csatorna
ICV	Intelligent Connected Vehicle	Intelligens kapcsolódó jármű
IEC	International Electrotechnical Commission	Nemzetközi Elektrotechnikai Bizottság
IEEE	Institute of Electrical and Electronics Engineers	Elektromérnökök és Elektronikai Mérnökök Intézete
IoT	Internet of Things	Dolgok Internete
ISO	International Organization for Standardization	Nemzetközi Szabványügyi Szervezet
JPEG	Joint Photographic Experts Group	Egyesült Fotótechnikai Szakértők Csoportja
MI	Mesterséges Intelligencia	Mesterséges intelligencia
MIIT	Ministry of Industry and Information Technology	Ipari és Informatikai Minisztérium
MQTT	Message Queuing Telemetry Transport	Telemetria üzenetsor protokoll
MST	Ministry of Science and Technology	Tudományos és Technológiai Minisztérium
NDRC	National Development and Reform Commission	Nemzeti Fejlesztési és Reformbizottság
NEOCC	New Energy and Oil Consumption Credits	Új energia és olajfogyasztási kreditek
NEV	New Energy Vehicle	Új energia jármű

NHTSA	National Highway Traffic Safety Administration	Országos Közúti Közlekedésbiztonsági Hivatal
NIS2	Network and Information Security Directive	Hálózati és információbiztonsági irányelv
NIST	National Institute of Standards and Technology	Országos Szabványügyi és Technológiai Intézet
OBD	On-Board Diagnostic	Fedélzeti diagnosztika
OEM	Original Equipment Manufacturer	Eredeti berendezésgyártó
OTA	Over the Air	Vezeték nélküli frissítés
PCM	Pulse Code Modulation	Impulzuskód-moduláció
PEV	Plug-in Electric Vehicle	Plug-in elektromos jármű
PHEV	Plug-in Hybrid Electric Vehicle	Plug-in hibrid elektromos jármű
PNG	Portable Network Graphics	Hordozható hálózati grafika
QoS	Quality of Service	Szolgáltatási minőség
RGB	Red Green Blue	Vörös-zöld-kék
SAE	Society of Automotive Engineers	Járműipari Mérnökök Társasága
SIM	Subscriber Identity Module	Előfizetői azonosító modul
SMS	Short Message Service	Rövid szöveges üzenet szolgáltatás
SOTIF	Safety of the intended functionality	A tervezett funkcionalitás biztonsága
TISAX	Trusted Information Security Assessment Exchange	Megbízható információbiztonsági értékelési csereprogram
TS	Technical Specification	Műszaki specifikáció
UNECE	United Nations Economic Commission for Europe	Egyesült Nemzetek Európai Gazdasági Bizottsága
V2I	Vehicle to Infrastructure	Jármű és infrastruktúra közötti kommunikáció
V2V	Vehicle to Vehicle	Járművek közötti kommunikáció
VoIP	Voice Over Internet Protocol	Internetprotokoll alapú hangátvitel
WAV	Waveform Audio File Format	Hullámforma audifájl-form
Wi-Fi	Wireless Fidelity	Vezetéknélküli megbízhatóság