ÓBUDAI EGYETEM
ÓBUDA UNIVERSITY

DOKTORI (PHD) ÉRTEKEZÉS

HEGYI HENRIETTA

Internetkapcsolatra képes személygépjárművek információs rendszereinek biztonsági vizsgálata

Témavezető: Dr. Erdődi László

BIZTONSÁGTUDOMÁNYI DOKTORI ISKOLA

Budapest, 2025.11.16.

Nyilvános védés teljes bizottsága:

Elnök:

Prof. Dr. Ludányi Laufer Edit

Titkár:

Dr. Kail Eszter

Tagok:

Dr. Muha Lajos

Dr. habil. Fleiner Rita

Dr. habil. Orosz Gábor Tamás

Bírálók:

Prof. Dr. Tick Andrea

Dr. habil. Krasznay Csaba

Nyilvános védés időpontja:

2026

NYILATKOZAT

A MUNKA ÖNÁLLÓSÁGÁRÓL, IRODALMI FORRÁSOK MEGFELELŐ MÓDON TÖRTÉNT IDÉZÉSÉRŐL

Alulírott Hegyi Henrietta kijelentem, hogy az *„Internetkapcsolatra képes személygépjárművek rendszereinek biztonsági vizsgálata”* című benyújtott doktori értekezést magam készítettem, és abban csak az irodalmi hivatkozások listáján megadott forrásokat használtam fel. Minden olyan részt, amelyet szó szerint, vagy azonos tartalomban, de átfogalmazva más forrásból átvettem, a forrás megadásával egyértelműen megjelöltem.

Budapest, 2025.11.16.

Hegyi Henrietta

TARTALOM

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 (akár megfelelő tájékoztatás nélkül) 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 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 [4], 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) [5].

Az internetre kapcsolódni képes személygépjárművek működése során az adatok folyamatos áramlása valósul meg a jármű és különböző külső rendszerek – például a gyártói szerverek, mobilalkalmazások, felhőszolgáltatások vagy infrastruktúraelemek – között. Ezzel a jármű az adatfeldolgozás aktív szereplőjévé válik, miközben érzékeny információk (pl. helyadatok, viselkedési mintázatok, kommunikációs preferenciák) folyamatosan generálódnak és potenciálisan hozzáférhetővé válnak. Az ilyen adatáramlás kockázatokat hordoz magában, különösen akkor, ha nem világos, ki fér hozzá ezekhez az információkhoz, milyen célból és milyen feltételekkel.

Noha az adatvédelmi és információbiztonsági alapelvek, mint a célhoz kötöttség, az adattakarékosság és az átláthatóság elviekben érvényesíthetők lennének, ezek gyakorlati alkalmazása sok esetben hiányos vagy formális. A probléma súlyosbodik azzal, hogy a járművezetők többsége nem rendelkezik kellő ismerettel az adatok útjáról, vagy nem is kap tájékoztatást arról, hogy az általuk használt jármű milyen adatokat oszt meg – és kivel. A szabályozási környezet e problémák kezelésére elvben alkalmas eszköz lehetne, azonban a jelenlegi európai és nemzetközi normarendszer rendkívül sokrétű, széttöredezett és eltérő alkalmazási mélységű. Az egymással párhuzamosan létező jogszabályok, iparági szabványok és ajánlások sok esetben csak keretjellegű előírásokat tartalmaznak, konkrét végrehajtási útmutatásokat ritkán. Ez a heterogenitás megnehezíti az érintettek számára annak megítélését, hogy pontosan milyen kötelezettségek és elvárások vonatkoznak rájuk az információbiztonság és adatvédelem terén. Mindez nemcsak a piaci szereplők jogbiztonságát gyengíti, hanem akadályozza az egységes, hatékony és számonkérhető biztonsági gyakorlatok kialakulását is.

1.2. Járműadat-ökoszisztémák és az internetkapcsolatra képes járművek környezetének szakirodalmi háttere

Az internetkapcsolattal rendelkező személygépjárművek megjelenése alapjaiban formálja át a közlekedés és az adatkezelés ökoszisztémáját. Az intelligens közlekedési rendszerek (ITS) fejlődésével a járművek már nem csupán közlekedési eszközként, hanem aktív adatgyűjtő, -feldolgozó és -továbbító egységként is működnek, ezzel új adatforrásként és információs csomópontként szolgálva a városi és országos infrastruktúrában [6],[7]. A modern személygépjárművek képesek meteorológiai, infrastrukturális és forgalmi adatokat gyűjteni, amelyeket nemcsak saját működésük optimalizálására, hanem más rendszerekkel, például városüzemeltetési vagy forgalomirányítási szervezetekkel is megoszthatnak [6],[7],[8].

A szakirodalom hangsúlyozza, hogy a jármű mint adatfeldolgozó egység védelme már az intelligens ITS rendszerek teljes körű megvalósulása előtt is kiemelt jelentőségű [6],[7],[9]. A személygépjármű ugyanis nem csupán egyéni adatvédelmi szempontból kritikus, hanem potenciális támadási felületet is jelent a teljes közlekedési infrastruktúra számára [10],[11],[12]. Ezzel párhuzamosan, az 5G alapú kommunikációs rendszerek és a V2X (Vehicle-to-Everything) technológiák terjedése tovább fokozza az adatbiztonsági és adatvédelmi követelmények súlyát [13],[14],[15].

Az internetkapcsolatra képes járművek környezetében a szereplők köre folyamatosan bővül: a gyártók és közvetlen szolgáltatók mellett egyre nagyobb jelentőséggel bírnak a városüzemeltetők, márkaszervizek, biztosítók, flottakezelők és mobilitási szolgáltatók [16]. Ezek a szereplők gyakran jogosultak vagy érdekeltek az egyes járműadatok elérésében, felhasználásában, illetve feldolgozásában [8]. Mindezek következtében a járműadat-ökoszisztéma sokszereplős és dinamikus, ahol a jogosultságok, felelősségi körök és adatáramlás szabályozása különösen összetett [16],[17].

A szabályozási környezet töredezettsége is jól látható: jelenleg nincs olyan egységes, részletesen kidolgozott nemzetközi szabvány vagy iránymutatás, amely pontosan meghatározná, hogy ezekkel a további szereplőkkel milyen típusú adatokat, milyen jogcímen, milyen céllal és feltételekkel lehet vagy kell megosztani [17]. Bár a GDPR általános adatvédelmi keretet biztosít, a járműadat-ökoszisztéma sajátosságait (pl. adatok valós idejű áramlása, szereplők közötti folyamatos jogosultságváltás) nem fedi le teljes körűen. A gépjárművezetők tájékoztatása is rendszerint hiányos: sok esetben nem egyértelmű számukra, hogy milyen adatokat oszt meg járművük, kivel és milyen céllal, miközben a hozzájárulásuk gyakran csak formális, például általános szerződési feltételekbe ágyazva történik [8],[16]. A szakirodalom és a szabályozási dokumentumok egyaránt rámutatnak, hogy mindaddig, amíg az adatmegosztási gyakorlatok, jogosultságok és a felhasználók információs jogai nem kerülnek átlátható és szabványosított formában rögzítésre, nem várható el a bizalom és az adatbiztonság magas szintje az okosjármű-ökoszisztémában [17].

A járművek által generált adatmennyiség és a kapcsolódó adatfeldolgozási technológiák is gyorsan fejlődnek. Stocker és munkatársai a „Quantified Vehicles” koncepcióban arra mutatnak rá, hogy egyetlen jármű CAN-buszon keresztül óránként akár 500 MB adatot is előállíthat, amelynek feldolgozása és hasznosítása új, adatplatform-alapú szolgáltatásokat tesz lehetővé az életciklus egészében [18]. Az adatgyűjtési és adatvédelmi kihívásokat modern jármű-operációs rendszerek, például az Android Automotive OS példáján keresztül is vizsgálják, kiemelve az egyre komplexebb adatgyűjtési mechanizmusokat és az ezekhez kapcsolódó privacy-kockázatokat [19]. Alam (2024) összefoglaló tanulmányában bemutatja, hogy az autonóm és csatlakoztatott járművek milyen új adatvédelmi és adatbiztonsági problémákkal szembesülnek [20], míg Yuca és szerzőtársai a privacy-preserving adatfeldolgozási módszerek, például a több fél közötti számítás

(MPC) vagy a homomorfikus titkosítás alkalmazási lehetőségeit hangsúlyozzák az autóiparban [21].

Az internetkapcsolatra képes személygépjárművek által generált és kezelt adatok mennyisége, feldolgozási módjai, valamint az adatkezelésbe bevont szereplők köre gyors ütemben bővül. Ez a sokszínű és gyorsan változó ökoszisztéma új szabályozási, technológiai és adatvédelmi kihívásokat jelent, amelyekre a jelenlegi szakirodalom, valamint a szabályozási és technológiai gyakorlat még nem tudott teljes körű választ adni. A dolgozat ezeknek a problémáknak a feltárását és rendszerezését tűzi ki célul.

1.3. A tudományos probléma megfogalmazása

Az internetkapcsolatra képes személygépjárművek (connected cars) megjelenése az autóipar digitalizációs átalakulásának egyik legmarkánsabb tünete. E járművek működése során valós idejű, kétirányú adatkommunikáció valósul meg a gyártói infrastruktúrák, szolgáltatók, felhőalapú rendszerek és – egyre gyakrabban – más járművek vagy közlekedési elemek irányába. Ennek következtében a személygépjármű funkcionális szerepe túllép a klasszikus közlekedési eszköz keretein: a jármű egyben informatikai rendszerként is értelmezhető, amelyben adatfeldolgozási, döntéshozatali és hálózati kommunikációs elemek működnek együtt. E fejlemény azonban számos új, gyakran nehezen körülhatárolható biztonsági és adatvédelmi kérdést is felvet.

A keletkező adatok jellege – például a helymeghatározás, vezetési szokások, felhasználói interakciók – és az ezekhez való hozzáférés lehetősége új típusú kockázatokat teremt a felhasználók számára. Ezen kockázatok értelmezése és kezelése a szabályozási szinttől a technológiai megvalósításon át a felhasználói tudatosságig több szinten vet fel kihívásokat. Különösen problémás, hogy az érintettek gyakran nem, vagy csak korlátozott módon kapnak tájékoztatást az adatkezelés részleteiről, miközben a technológia egyre összetettebbé és autonómabbá válik.

A jogi és szabályozási keretrendszerek az elmúlt években jelentős fejlődésen mentek keresztül, azonban jelenleg is egy széttöredezett, sokszor csak keretjellegű és eltérő mélységű elvárásokat megfogalmazó környezetként értelmezhetők. Egyes szabályozások elsősorban adatvédelmi, mások kiberbiztonsági, megint mások szervezeti megfelelőségi szempontokat hangsúlyoznak. E sokszínűség – bár alapvetően előremutató – nehezíti a követelmények egységes értelmezését és összehangolt alkalmazását, különösen egy olyan összetett rendszer esetén, mint az autóipari ökoszisztéma.

Ezen túlmenően a járművek hálózati architektúrája és a kommunikációs protokollok sajátosságai olyan kérdéseket is felszínre hoznak, amelyekre a szabályozási dokumentumok csak áttételesen reagálnak. Az információáramlás átláthatósága, a technikai korlátokból adódó sebezhetőségek, valamint a potenciálisan nem szándékolt adatáramlási útvonalak problémája mind olyan jelenségek, amelyek komplex megközelítést igényelnek – és amelyekre a jelenlegi szabályozási és technológiai válaszok nem minden esetben adnak kielégítő megoldást.

A tudományos probléma tehát egy olyan – technológiai, jogi és társadalmi szempontból egyaránt rétegzett – kihívás köré épül, amely az internetkapcsolatra képes járművek működésének biztonsági aspektusait kívánja rendszerszinten értelmezni. A kutatás célja, hogy hozzájáruljon e kérdéskör jobb megértéséhez, valamint rámutasson azokra a pontokra, ahol a szabályozási szándék és a gyakorlati működés között diszkrepancia mutatkozik.

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 [22]. 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 [23].

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 [24].

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 [28].

1.4. A kutatás tudományos újdonsága és szükségszerűsége

A kutatás újszerűsége abban rejlik, hogy a járműipari információbiztonságot holisztikus megközelítésben vizsgálja: a technológiai, szabályozási és társadalmi dimenziókat egymással összefüggő rendszerelemeknek tekinti, nem pedig elszigetelt szakterületeknek. A meglévő szakirodalom döntő többsége egy-egy részterületre – például a hálózati protokollokra vagy a felhasználói magatartásra – fókuszál, így nem képes feltárni a teljes ökoszisztéma összefüggéseit. Ez a tudományos töredezettség a gyakorlatban is megjelenik: a szabályozási és iparági gyakorlatok sokszor elszigetelten kezelik a problémákat, ami akadályozza a követelmények egységes értelmezését és alkalmazását. A jelen kutatás ezzel szemben integrált módon vizsgálja az adatbiztonsági kihívásokat, feltárva a szereplők – gyártók, szabályozó hatóságok, felhasználók – közötti kölcsönhatásokat és a széttöredezett gyakorlat mögötti szerkezeti okokat.

A tudományos szükségszerűséget az indokolja, hogy az internetkapcsolattal rendelkező járművek új típusú, a teljes életcikluson át fennálló kiberbiztonsági kockázatokat hordoznak. A hagyományos járműbiztonsági modellek nem alkalmasak a szoftveralapú, távoli hozzáférésre képes rendszerekből eredő fenyegetések kezelésére. Az Európai Unió jelenlegi szabályozási környezete hiányos és széttöredezett, miközben más globális szereplők – például Kína – eltérő szabályozási és végrehajtási logikákat követnek. E különbségek összehasonlító vizsgálata, valamint az iparági sztenderdek (például ISO/SAE 21434) kritikai elemzése hozzájárulhat egy hatékonyabb, külső ellenőrzéssel támogatott kockázatkezelési modell kialakításához.

A kutatás további újdonsága, hogy empirikus felmérések révén feltárja a felhasználói percepciókat és azok hatását a biztonságra. Eredményei rávilágítanak, hogy a fogyasztók a kockázatokat sokszor alábecsülik vagy figyelmen kívül hagyják – részben az elégtelen tájékoztatás, részben a technológiai fejlődés iránti bizalom miatt. Ez a magatartás komoly nemzetbiztonsági kockázatot jelenthet, különösen, ha a sérülékenységek flottaszintű adatgyűjtést vagy megfigyelést tesznek lehetővé. A dolgozat technikai vizsgálatokkal is alátámasztja ezt: bemutatja, miként válhatnak a járművek kommunikációs protokolljai rejtett adatcsatornák hordozóivá, amelyek a hagyományos titkosítási és hálózatbiztonsági megoldások mellett is kihasználhatók.

A kutatás tehát multidiszciplináris módon járul hozzá az internetkapcsolatra képes járművek információbiztonsági szabályozásának, kockázatelemzési módszertanának és

felhasználói aspektusainak mélyebb megértéséhez. Célja egy olyan átfogó, nemzetbiztonsági szempontokat is figyelembe vevő védelmi logika megalapozása, amely képes egységes keretbe foglalni a technológiai, jogi és társadalmi dimenziókat, illetve a új kutatási irányok megfogalmazásának az alapját képezheti az érintett a tématerületeken belül.

1.5. A téma aktualitása

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.

1.5.1. Kína térnyerésének hatása az európai személygépjárműipar információbiztonságára

Kína vizsgálatának kiemelt kezelése több, egymást erősítő tényezőn alapul. Az ország az elmúlt két évtizedben a világ egyik legnagyobb autóipari és technológiai szereplőjévé vált, jelentős részesedéssel mind a járműgyártásban, mind a kapcsolódó digitális infrastruktúrák fejlesztésében. Ezzel párhuzamosan a kínai szabályozási környezet

sajátos, központilag vezérelt jellege és gyors alkalmazkodóképessége éles kontrasztot mutat az európai és észak-amerikai modellekkel, ami lehetővé teszi a különböző megközelítések összehasonlítását. Továbbá Kína nemcsak exportpiaci, hanem technológiai befolyása is folyamatosan növekszik, ami a nyugati járműpiacok ellátási láncaira és biztonsági kockázataira közvetlen hatást gyakorol. A következő alfejezetekben bemutatott statisztikai adatok és iparági trendek alátámasztják, hogy Kína szerepe e kutatás kontextusában nem pusztán releváns, hanem kulcsfontosságú.

Az Európai Unióba importált elektromos és intelligens járművek között a kínai márkák aránya évről évre nő, aminek több dimenzióban is jelentősége van: egyrészt a digitális architektúra és a kommunikációs protokollok gyakran nem transzparens módon kerülnek integrálásra ezekben a járművekben, másrészt a gyártók adatkezelési gyakorlata sok esetben kívül esik az uniós adatvédelmi és információbiztonsági normarendszeren.

A kínai gyártmányú okosautók terjedése így nem csupán piaci vagy technológiai, hanem stratégiai és biztonsági kérdéseket is felvet. A kapcsolt járművek távoli elérésének, szoftverfrissítési mechanizmusainak és szenzoradataihoz való hozzáférésének kockázatai különösen érzékennyé válnak abban az esetben, ha ezen rendszerek felett olyan joghatóságú szereplők rendelkeznek, amelyek nem kötelesek az európai adatvédelmi és kibervédelmi szabványok betartására, vagy ahol a szabályozás eltérő értelmezése gyengébb garanciákat nyújt.

Az Európai Unió az elmúlt években jelentős lépéseket tett az információbiztonság és az adatvédelem terén. Ennek legismertebb példái a GDPR és a NIS2 irányelv, amelyeket az uniós tagállamok már beépítettek saját jogrendjükbe. Ugyanakkor ezek a szabályozások elsősorban az EU területén működő szervezeteket érintik, a harmadik országokból származó gyártókkal szembeni betartatásuk azonban nehézkes [26]. Ez a probléma különösen hangsúlyos Kína esetében, amely jelentős piaci térnyerést ért el Európában az elektromos járművek terén.

A jelen fejezetben leírt jelenség hátterének magyarázatával külön publikációban foglalkoztam. A jelenség hátterét részletesen feldolgoztam korábbi tanulmányomban [27], amely a kínai gyártású elektromos személygépkocsik európai elterjedésének biztonsági kockázatait vizsgálta. A kutatás bemutatta, hogy a kínai állam által évtizedek óta következetesen támogatott villamosjármű-ipar stratégiai jelentőségűvé vált, és az utóbbi években célzottan erősítette jelenlétét az uniós piacon. A járművek által gyűjtött

és távolról feldolgozott adatok – a szenzorhálózatok, fedélzeti rendszerek és hálózati protokollok révén – érzékeny személyes és infrastrukturális információkat is magukban foglalhatnak. A tanulmány kvalitatív módszerekkel, tíz információbiztonsági szakértő bevonásával azonosította azokat a szabályozási hiányosságokat, amelyek nemzetbiztonsági kockázatot eredményezhetnek, különösen akkor, ha az adatok harmadik országba kerülnek feldolgozásra. A kutatás arra a következtetésre jutott, hogy a jelenlegi uniós szabályozási környezet – bár fejlődőképes – nem képes teljes körűen kezelni a harmadik országból származó, internetkapcsolatra képes járművek adatbiztonsági kihívásait, ezért a témakör kiemelt figyelmet érdemel.

Az európai uniós új gépjármű-regisztrációk terén a kínai márkák piaci térhódítása jelentős mértékű növekedést mutatott 2023 és 2025 első felében. JATO Dynamics adatai szerint:

2023-ban a kínai márkák piaci részesedése elérte az 2,5 %-ot az EU teljes piacán [28]. 2024-ben ez az arány tovább emelkedett, és éves szinten meghaladta a 4 %-ot [29]. 2025 májusában, tehát legfrissebb vizsgálati adatok alapján, már 5,9 %-ot tett ki (65 808 regisztráció), ami több mint kétszerese a tavalyi 2,9 %-os szintnek ugyanebben a hónapban [30],[31]. 2025 januárjában pedig 37 134 kínai jármű kapott új forgalmi engedélyt az EU-ban, ami 3,7 %-os részesedést jelent (a 2024. januári 2,4 %-hoz képest) [32].

A kínai gyártók térnyerését nemcsak az új regisztrációk arányának alakulása jelzi, hanem az is, hogy egyes vállalatok már a tíz legnagyobb európai szereplő közé is bekerültek. A számszerű adatokat az 1. Számú mellékletben található táblázat szemlélteti.

Az alternatív hajtású járművek tekintetében a kínai márkák különösen erősek: 2025 januárban az összes hibrid (HEV) regisztráció 6,1 %-át, a plug-in hybrid (PHEV) kategóriában pedig 4 %-át tették ki [33]. Az európai piac ugyancsak megfigyelhető trendeket mutat a márkák szintjén: több kínai gyártó – köztük a BYD, MG/SAIC, Chery, Geely, Xpeng – egyre aktívabbá vált. 2025 áprilisban a BYD először előzte meg a Teslát az európai BEV-eladásokban (7 231 vs. 7 165 darab) [34], [35], míg májusban a kínai márkák összesített piaci részesedése elérte az 5,9 %-ot [30], [35].

Az európai szabályozási környezet sem maradt változatlan: az EU 2024 júliusától 0–38 % közötti vámokat vezetett be a Kínából érkező elektromos autókra, amelyek a vizsgálatfüggő, piaci beavatkozás eredményeként léptek életbe [36],[37]. Ennek ellenére a kínai márkák piaci térnyerése folytatódott – Kína újabb kaput nyitott Európára.

Kína elektromos személygépjármű-iparának gyors fejlődése nem véletlenszerű, hanem tudatos állami stratégia eredménye. Az elmúlt évtizedben számos állami program, köztük jelentős kutatás-fejlesztési támogatások és piaci ösztönzők révén Kína globálisan vezető szereplővé vált az elektromos járművek piacán [38]. A kínai elektromos járművek nemcsak technológiai fejlettségük miatt jelentenek kihívást Európának, hanem azért is, mert ezek a járművek nagy mennyiségű adatot gyűjtenek a felhasználókról, beleértve érzékeny személyes adatokat és pontos helyinformációkat [39].

Az európai piacon megjelenő kínai elektromos járművek relatíve alacsony áruk miatt vonzóak a vásárlók számára, ugyanakkor információbiztonsági szempontból problémásak lehetnek. A kínai adatkezelési gyakorlat és jogszabályi környezet jelentősen eltér az európaitól, a kínai gyártók működését pedig jelentős állami befolyás jellemzi [40]. A jelenlegi európai szabványok, mint az ISO/SAE 21434 vagy a TISAX, nem elegendőek ahhoz, hogy megfelelően ellenőrizzék és betartassák az EU-n kívüli gyártók információbiztonsági gyakorlatát, különösen a komplex beszállítói láncokon keresztül érkező termékek esetében.

A problémát súlyosbítja, hogy Kína állami politikája explicit módon támogatja az adatok széleskörű gyűjtését, ami felveti annak lehetőségét, hogy a gyűjtött adatok – megfelelő kontroll nélkül – harmadik felekhez vagy akár állami szervekhez kerülhetnek [41]. Ez különösen érzékeny kérdés az Európai Unió számára, hiszen egy ilyen jellegű adatáramlás nemcsak az állampolgárok személyes adatainak biztonságát veszélyeztetheti, hanem szélesebb értelemben vett nemzetbiztonsági kockázatokat is hordozhat [42].

Az Európai Uniónak ezért sürgető szüksége lenne olyan intézkedésekre, amelyekkel egységes és hatékony módon képes kezelni a harmadik országból, különösen Kínából érkező információbiztonsági kihívásokat. Ehhez elengedhetetlen lenne egy egységes audit- és tanúsítási rendszer kialakítása, amely nemcsak a gyártókra, hanem azok beszállítói láncaira is kiterjed [43].

1.6. Célkitűzések

Az információbiztonság növekvő szerepe a modern személygépjárművek működésében arra ösztönzött, hogy összevessem az ismert fenyegetéseket a szabályozások tartalmával és céljaival. A kutatás célja annak vizsgálata, hogy a jelenlegi szabályozási 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:

1. Az európai szabályozási környezet elemzése az internetkapcsolattal rendelkező személygépjárművek kiberbiztonságának szempontjából, annak feltárására, hogy a jelenlegi szabályozási keretrendszer képes-e átfogó és egységes védelmet biztosítani a releváns fenyegetésekkel szemben.
2. A szabályozásokban megjelenő kockázatelemzési megközelítések vizsgálata, különös tekintettel arra, hogy ezek mennyire képesek lefedni az internetre kapcsolt járművek teljes életciklusát és a különböző érintetti szinteket (jármű, szervezet, ökoszisztéma).
3. A járműhasználók tudatossági szintjének feltérképezése a járművek hálózati funkcióival és azok biztonsági kockázataival kapcsolatban, valamint annak vizsgálata, hogy a jelenlegi edukációs és tájékoztatási mechanizmusok elegendőek-e a kockázatok felismeréséhez.
4. A járműkommunikációban alkalmazott protokollok vizsgálata abból a szempontból, hogy lehetővé teszik-e rejtett kommunikációs csatornák kialakítását, és ha igen, milyen műszaki és szabályozási eszközök szükségesek ezek felismeréséhez és kezeléséhez.
5. Egy modell kidolgozása és validálása, amely képes kimutatni, hogy az internetre kapcsolt, fejlett vezetéstámogató rendszerekkel rendelkező járművek miként válhatnak érzékeny adatok rejtett továbbítására alkalmas eszközökké, és milyen biztonságpolitikai vagy nemzetbiztonsági következményei lehetnek ennek flottaszinten.

A kutatási 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.

1.7. Kutatási kérdések

A kutatás megkezdése előtt egy-egy jól körülhatárolható kutatási kérdést fogalmaztam meg. Ezek a kérdések segítettek strukturálni a vizsgálati irányokat és meghatározni az alkalmazott módszertani megközelítéseket.

1. K1: Milyen mértékben képes az Európai Unió jelenlegi szabályozási keretrendszere hatékony védelmet nyújtani az internetkapcsolattal rendelkező személygépjárművekkel szemben fennálló információbiztonsági fenyegetések ellen?
2. K2: Milyen korlátai vannak a jelenleg alkalmazott járműipari kockázatelemzési módszereknek az internetkapcsolattal rendelkező járművek komplex információbiztonsági kockázatainak kezelésében?
3. K3: Milyen mértékben tájékozottak az internetkapcsolattal rendelkező járművek vásárlói a biztonsági kockázatokról, és ez hogyan befolyásolja döntéshozatalukat a járművásárlás során?
4. K4: Alkalmasak-e az internetkapcsolatra képes járművek kommunikációs protokolljai rejtett csatornák kialakítására, és milyen mértékben nyújthatnak védelmet ezek ellen a hagyományos technikai biztonsági intézkedések?
5. K5: Milyen módon használhatók fel az internetkapcsolattal rendelkező járművek szenzor- és kommunikációs adatai kijelölt objektumok vagy célszemélyek rejtett megfigyelésére, és ez milyen nemzetbiztonsági kockázatokat hordoz flottaszinten?

1.8. A kutatás felépítése

A disszertáció szerkezete egymásra épülő, tematikus fejezetekből áll, amelyek a kutatás főbb irányait, kérdéseit és módszertani lépéseit követik. Az első fejezetek a témaválasztás indoklását, a szakirodalmi hátteret, a tudományos problémát, újdonságokat, célkitűzéseket és a kutatási kérdéseket mutatják be. Ezt követően részletesen ismertetem a kutatás során alkalmazott módszertant, mely kvalitatív (pl. dokumentumelemzés, tematikus és keretelvű tartalomelemzés, szakértői interjúk) és kvantitatív (kérdőíves felmérés) elemeket is tartalmaz.

A dolgozat fő fejezeteiben először az autóipari szabályozási környezet, majd az empirikus kutatás eredményei (felhasználói kérdőív és szakértői interjúk) kerülnek bemutatásra. Ezek után következik a kommunikációs protokollok és az adattovábbítás mennyiségi

modellezésének elemzése, különös hangsúlyt fektetve a rejtett csatornákra és azok biztonsági kockázataira. A munka zárásaként átfogó kockázatelemzési modellt vázolok fel, amely a hatósági felügyelet lehetőségeit is figyelembe veszi.

A kutatás felépítése így lehetővé teszi a személygépjárművek információbiztonsági kihívásainak komplex, interdiszciplináris megközelítését, mind a szabályozási, mind a technológiai, mind a felhasználói szempontok alapján.

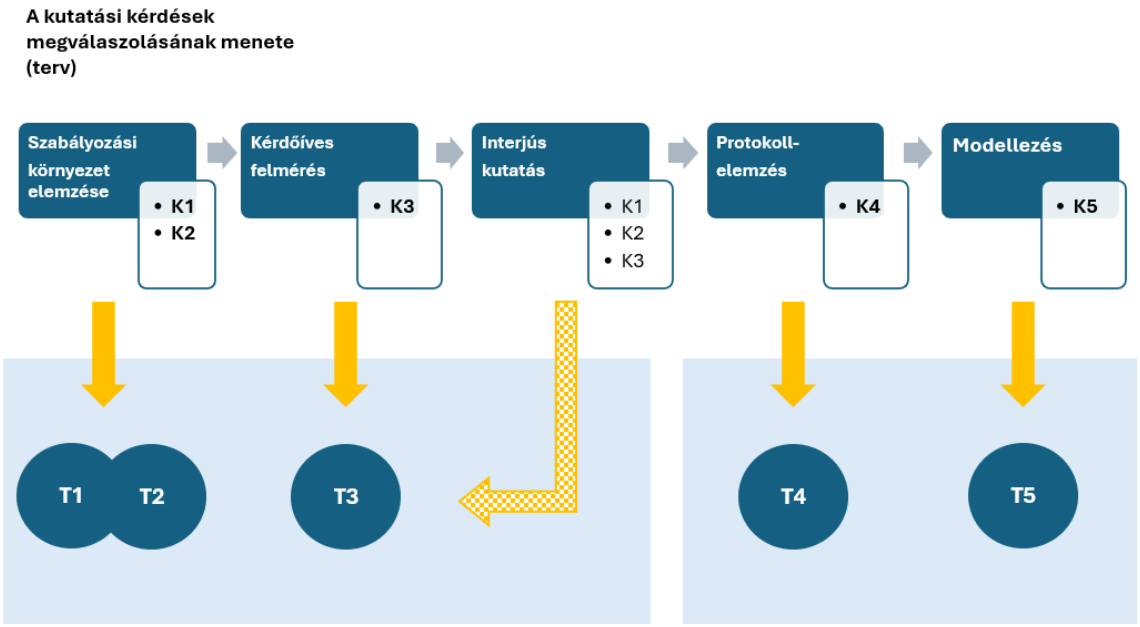
2. KUTATÁSI MÓDSZERTAN

A kutatás kezdeti szakaszában arra törekedtem, hogy a vizsgálatot logikus, egymásra épülő módszertani lépések szerint szervezzem. Úgy gondoltam, hogy a kutatási kérdések lineárisan, jól körülhatárolható szakaszokon keresztül válaszolhatók meg, ahol minden módszer egy-egy konkrét problémakörhöz vagy tézishez kapcsolódik.

A dolgozat módszertani kereteit ennek megfelelően az alábbi főbb megközelítések alkotják:

- **Szabályozási környezet elemzése:** Kvalitatív dokumentumelemzés, tematikus és keretelvű tartalomelemzés, funkcionális összehasonlítás – a jogszabályi és szabványi környezet rendszerszintű, kritikus vizsgálata céljából.
- **Empirikus kutatások:** Kvantitatív kérdőíves felmérés a végfelhasználók információbiztonsági tudatosságának, illetve attitűdjeinek feltárására, valamint kvalitatív, félig strukturált szakértői interjúk az iparági szereplők és szabályozók tapasztalatainak, értelmezéseinek és gyakorlati kihívásainak mélyebb megértéséhez.
- **Kommunikációs protokollok biztonsági elemzése:** A járművekben használt protokollok vizsgálata az OSI-modell rétegei mentén, fenyegetésmodellezéssel (pl. STRIDE), különös tekintettel a rejtett csatornákra és a privacy-kockázatokra.
- **Elméleti modellalkotás:** Az adattovábbítás, illetve megfigyelési potenciál mennyiségi modellezése, különböző szenzoradatok (kép, hang, helyzet) elemzése alapján.

Az 1. ábra szemlélteti, hogy eredetileg hogyan került megtervezésre a kutatási kérdések megválaszolása és a hozzájuk kapcsolódó módszertani lépések



1. ábra - A kutatási kérdések megválaszolásának tervezett menete. Forrás: saját forrás.

A kutatási folyamat tervezésekor abból indultam ki, hogy a fő kutatási kérdéseket lépésről lépésre, egymásra épülő vizsgálati szakaszokban tudom megválaszolni. Úgy gondoltam, hogy a szabályozási környezet elemzése ad majd választ az első két kérdésre (K1, K2), ezt követően a kérdőíves felmérés segít feltárni a felhasználói attitűdöket (K3), míg az interjús kutatás további kiegészítő bizonyítékokkal szolgálhat nemcsak a saját kutatási kérdéseihez, hanem a korábbiakhoz is. A protokollelemzés és a modellezés önálló, speciális tézisek kidolgozását tette volna lehetővé (T4, T5).

Az ábrán ezért a kutatási kérdések az egyes módszertani blokkokhoz kapcsolódva jelennek meg: vastag betűvel ott, ahol teljes körű válaszadást terveztem, vékony betűvel pedig ott, ahol csak kiegészítő, megerősítő adatokat kívántam gyűjteni az adott témához.

2.1. Fogalmi keretek

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 [44], [45].

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 [46].

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 [47] A jelenlegi technológiai trendek alapján tehát az összekapcsolt járművek két fő adatkapcsolati típussal rendelkezhetnek. Ezeket a 2. számú melléklet 12. táblázatában szemléletem.

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 [48].

Az "okosautó" és a korábbiakban használt "connected car" vagy összekapcsolt autó fogalom gyakran együtt jelennek 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 – így én is szinonimaként alkalmazom őket –, de ezzel egyidőben egyes értelmezések szerint fontos különbségek is lehetnek közöttük. Ezeket a különbségeket a 2. Sz. Melléklet 13. Definíciós táblázatában mutatom be.

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*[1] 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*[2]) 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 [51]. Bár a legtöbb esetben a támadóknak nem feltétlenül céljuk a járműben tartózkodók életének közvetlen

[1] 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.

[2] 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.

veszélyeztetése – hiszen a távolról történő, élet elleni támadások technikai és jogi kockázata jelentős –, ugyanakkor az adatok gyűjtése, a felhasználók profilozása, valamint a gépjármű szenzoraiból származó jelekkel a külső környezet monitorozása sokkal jövedelmezőbb tevékenységet jelenthet a támadók számára. A rengeteg gyűjtött adatnak köszönhetően egy sikeres behatolás nagy anyagi haszonnal kecsegtethet, amely tovább növeli a személyes és adatbiztonsági kockázatokat [52]. 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 [53], [54].

Szintén fontos fogalmak az adatbiztonság és az adatvédelem. A két fogalom jelentése szorosan összefügg, mégis fontos különbséget tenni köztük, különösen információbiztonsági kontextusban, ezért a 2. Sz. Melléklet definíciós táblázatai között az 14. Táblázatban összefoglaltam, milyen jelentéstartalommal jelennek meg az értekezésben. Az okosautó és internetkapcsolatra képes autó fogalmakkal ellentétben nem felcserélhetőek.

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

A kutatás szempontjából érdemes még kitérni a soft privacy (magyarul: puha magánszféra-védelem vagy lágy adatvédelem) fogalomra. A soft privacy mint fogalom a 2000-es évek végén jelent meg a szakirodalomban. George Danezis 2007-ben egy műhelyelőadásában vezette be először a „hard” és „soft” privacy közti különbségtételt [55]. A fogalmat később Mina Deng és munkatársai formalizálták 2011-es publikációjukban, amikor egy privacy fenyegetésmodellezési keretrendszert ismertetve különböztették meg a privacy technológiák két típusát [56]. Elterjedése a 2010-es évek közepére tehető a kutatásokban, válaszul arra, hogy az egyre növekvő számú IoT-eszköz (különösen az okosjárművek, okosórák és okosotthonok rendszerei) masszív mennyiségű adatot generálnak, amelyek bár nem feltétlenül személyazonosítók, mégis alkalmasak lehetnek érzékeny következtetések levonására. A soft privacy-fenyegetések leginkább a személyek tartózkodási helyéhez, útvonalaihoz, hangutasításaihoz, közeli eszközeinek listájához vagy vezetési stílusához kapcsolódnak.

A lágy adatvédelem legfontosabb jellemzője, hogy az érintett személy lemond az adatok közvetlen ellenőrzéséről, és az adatkezelő felelősségére bízza azok védelmét [56], [57]. A soft privacy kifejezetten olyan mechanizmusokra vonatkozik, amelyek biztosítják, hogy a felhasználó hozzájárulásával történjen az adatkezelés, és hogy utólagos jogorvoslatra is lehetőség legyen. A soft privacy tehát nem az adatkiadás megelőzésére, hanem annak felelős és átlátható kezelésére koncentrál [57] – ennek az elvnek azonban a gyakorlati érvényesülése számos esetben korlátozott, és nem mindig felel meg az elvárható szintnek.

Másrészt, a visszaélések oldaláról megközelítve a soft privacy kifejezés a magánszféra olyan fenyegetettségeire is utal, amelyek nem közvetlen adatlopás vagy klasszikus kibertámadás formájában jelentkeznek, hanem finomabb, közvetett módon veszélyeztetik az egyén információs önrendelkezését. Ezek az esetek tipikusan olyan adatok aggregálásából erednek, amelyek elsőre nem tűnnek érzékenynek, de viselkedésminták, mozgásprofilok vagy szokások alapján utólag rekonstruálhatóvá teszik az egyén identitását, preferenciáit vagy életritmusát.

A soft privacy egyik legismertebb alkalmazási területe az autóipar, ahol 2023-ban Raciti és Bella kutatása [58] több mint húszféle ilyen fenyegetést azonosított, az egyszerű lokációs követéstől a mikrofonadatok nem tervezett elemzéséig. A kutatók kiemelik, hogy ezek a kockázatok gyakran kívül esnek a felhasználók kontrollján, ugyanakkor hosszú távon komoly hatással lehetnek a digitális önrendelkezésre és a bizalomra az adatvezérelt járműtechnológiákkal szemben.

Az okosautók elterjedésével és gyors evolúciójával párhuzamosan az európai piacon is egyre markánsabban kirajzolódnak azok a trendek, amelyek meghatározzák a jövő személygépjárműveinek biztonsági kihívásait. Egyre több olyan új, korábban ismeretlen szereplő jelenik meg az ökoszisztémában, akik tevékenysége közvetve vagy közvetlenül hatással van a járművek adatvédelmi és kiberbiztonsági kitettségére. Mindez azt jelzi, hogy az okosgépjárművek várhatóan a kiberbűnözők és egyes állami hátterű szereplők számára is növekvő vonzerőt jelentenek, ami hosszú távon különösen összetett fenyegetési környezet kialakulásához vezethet.

A Dolgok Internete, azaz az "Internet of Things" (IoT) kifejezést Kevin Ashton alkotta meg 1999-ben, egy előadáson a Procter & Gamble-nél [59]. Az IoT eszközök fogalmára

azóta többféle definíció is elterjedt, melyek közül néhány gyakran alkalmazottat a 2. Sz. Melléklet 15. táblázatában gyűjtöttem össze.

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 a korábban említett definícióknak megfelelnek. 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 [60]. Ezek a kihívások szintén megfigyelhetőek a személygépjárművek esetén.

2.2. Szabályozási környezet vizsgálatához alkalmazott módszertani megközelítések

A kutatás célja az internetkapcsolattal rendelkező személygépjárművek információbiztonsági szabályozási környezetének átfogó feltárása. Ennek érdekében több, egymásra épülő kvalitatív módszertant alkalmaztam, amelyek együttesen biztosították a szabályozások rendszerszintű és összehasonlítható elemzését. A vizsgálat alapját a kvalitatív dokumentumelemzés képezte, amely lehetővé tette a jogi szövegek, iparági szabványok és hatósági ajánlások strukturált vizsgálatát. A módszer segítségével feltárhatók a dokumentumok mögöttes szabályozási szándékai, hiányosságai és következményei [61], valamint az egyes előírások közötti koherencia vagy normatív ütközések [62]. A tematikus elemzés célja a szabályozások mögötti főbb témák és alapelvek azonosítása volt, míg a keretelvű elemzés ezek rendszerezését és összehasonlíthatóságát tette lehetővé. A két megközelítés eredményeit a funkcionális összehasonlító elemzés szintetizálta, amely a szabványok gyakorlati alkalmazhatóságát, lefedettségét és kockázatkezelési képességeit vizsgálta. E három módszertani szint

együttesen biztosította, hogy a kutatás feltárja a főbb szabályozási hiányosságokat, átfedéseket és ellentmondásokat, valamint átfogó képet adjon a járműipari szabályozási környezet működéséről.

2.2.1. Keretelvű elemzés (Framework Analysis)

A Framework Analysis előnye, hogy képes ötvözni a deduktív és induktív megközelítést: egyrészt egy előre definiált keretbe (framework) szervezi az adatokat, másrészt nyitott marad az új, előzetesen nem várt kategóriák befogadására. Ez a rugalmasság tette különösen alkalmassá a módszert a kutatási kérdések vizsgálatára, mivel a cél nemcsak az volt, hogy a meglévő iparági és szabályozási keretekhez igazítsuk a tapasztalatokat, hanem az is, hogy ezek hiányosságaira és fejlesztési lehetőségeire rámutassunk. A módszertan alkalmazásának célja az volt, hogy szisztematikus, reprodukálható módon azonosíthatóvá váljanak a szabályozások hiányterületei, illetve azok kapcsolódása a gyakorlati implementációhoz [64].

A módszertan öt kulcslépését követve végeztem az elemzést: (1) az adatokkal való megismerkedés, (2) a tematikus keret kialakítása, (3) indexelés, (4) adatok rendszerezése a keret szerint, (5) értelmezés és következtetések levonása. Az alkalmazott keretrendszer alapját a járműipari információbiztonsági szabványok (pl. ISO/SAE 21434) és az európai, valamint kínai szabályozások kulcselemei adták. A keret kiegészült a Thematic Analysis során feltárt, a gyakorlatban tapasztalt problémákkal, így a két módszer egymásra épülése biztosította az elemzés mélységét.

A Framework Analysis révén lehetővé vált a különböző szabályozási és iparági modellek rendszerszintű összehasonlítása, valamint azok erősségeinek és gyengeségeinek feltárása. Ez közvetlenül hozzájárult a kutatási kérdések megválaszolásához azáltal, hogy empirikus adatokkal és strukturált elemzéssel támasztotta alá a javasolt kockázatkezelési modell megalapozottságát.

2.2.2. Tematikus tartalomelemzés (Thematic Analysis)

Braun és Clarke (2006) [63] meghatározása szerint a tematikus elemzés rugalmas és széles körben alkalmazható kvalitatív kutatási módszer, amely különösen alkalmas visszatérő mintázatok és témák feltárására nagy terjedelmű szöveges anyagokban. A jelen szakasz célja, hogy a korábban végzett keretalapú és indexelő elemzéseket kiegészítve további nézőpontból értelmezze a releváns szabványokat és jogszabályokat, különös tekintettel azok tartalmi súlypontjaira és strukturális sajátosságaira. A tematikus elemzés

hatlépcsős metodikáját követve – adatismertetés, kódolás, kezdeti témák azonosítása, témák felülvizsgálata, témák megnevezése és az eredmények integrálása – törekszem olyan szabályozások beazonosítására, amelyek ténylegesen hozzájárulnak az értekezés 1. és 2. kutatási kérdéseinek vizsgálatához. Az ezekre vonatkozó későbbiekben megfogalmazott tézisek arra mutatnak rá, hogy az európai szabályozási környezet jelenleg nem nyújt átfogó és egységes védelmet az internetkapcsolattal rendelkező személygépjárművek ismert fenyegetéseivel szemben, valamint hogy a kockázatelemzési megközelítések nem fedik le teljes körűen a gyártói és szervezeti szinteket.

A dokumentumelemzést tematikus tartalomelemzéssel egészítettem ki, amely során előre definiált témakörök (pl. életciklus-fókusz, kockázatkezelési követelmények, végrehajthatóság) mentén történő kódolást végeztem. A tartalomelemzés célja az volt, hogy az egyes szabályozások strukturálható és összehasonlítható elemeit kiemelje, lehetővé téve a kvalitatív mintázatok feltérképezését [64]. A kódolás manuálisan történt, iteratív módon, a témák finomhangolása mellett.

2.2.3. Funkcionális összehasonlító elemzés

Az összehasonlító elemzés célja, hogy egységes, két-dimenziós, mátrixalapú keretben értékelje a vizsgált szabványokat és jogszabályokat (pl. UNECE WP.29 R155/R156, ISO/SAE 21434, ISO 26262, ISO/IEC 27001, NIST CSF, Cyber Resilience Act), és ezzel közvetlenül támogassa a K1–K2 kutatási kérdések megválaszolását. A keret azt vizsgálja, hogy az európai szabályozói környezet mennyire képes tényleges védelmet nyújtani a hálózatba kapcsolt járműveket érő fenyegetésekkel szemben (K1), illetve hol mutatkoznak módszertani korlátok a jelenlegi kockázatelemzési megközelítésekben (K2).

A dokumentumok két, egymást kiegészítő dimenzió mentén kerülnek összevetésre: normatív és technikai dimenzió mentén. A normatív dimenzió vizsgálata során a kötelező erő és végrehajthatóság komponensei (hatósági alap és hatály, szankcionálhatóság, felügyeleti mechanizmusok) kerülnek vizsgálat alá, amelyek a hard–soft law megkülönböztetésből vezethetők le [61], [62]. A technikai dimenzió elemzése során pedig a releváns támadási vektorok lefedettsége, különös tekintettel a távoli hozzáférési csatornákra, hálózati/protokollrétegre, firmware/bootláncra, érzékelői manipulációkra, járműbuszokra, ellátási láncra és a tárolt/személyes adatok védelmére; a kategóriák az ENISA közlekedési fenyegetési összképéből származnak [66]. A komparatív

megközelítés funkcionális jellegű, a dokumentumok tényleges szabályozói és műszaki hatására koncentrál [64]. A keresztmetszeti szabályozásértékelés indokoltságát az OECD RIA-elvek támasztják alá [67].

A két dimenzió részpontszámai egyszerű additív összegzéssel (Simple Additive Weighting, SAW) állnak össze súlyozás nélkül [65], a többkritériumos értékelések bevett gyakorlatához igazodva [68]. Az összpontszám 0–17-es skálára vetítve ad besorolást: 0–4 = Nem megfelelő; 5–8 = Alacsony erejű; 9–12 = Közepes erejű; 13–16 = Megfelelő; 17 = Ideális. A skála definíciója és a megfelelési térkép összhangban van a fejezet későbbi táblázataival és eredményeivel (lásd a következő alfejezet(ek) táblázatait).

Az eljárás lépései a következők:

1. Beválogatás: a járműipari relevancia és joghatósági jelentőség alapján célzottan kiválasztott dokumentumok (kötelező és önkéntes keretek vegyesen) [67].
2. Kritérium-hozzárendelés: a normatív és technikai dimenziók mérőszempontjainak rögzítése a fenti irodalmi alapok (hard/soft law; fenyegetési vektorok) szerint [61], [62], [66].
3. Pontozás és összegzés: a mátrix kitöltése, részpontszámok és SAW-alapú összpontszám képzése súlyozás alkalmazása nélkül [65], [68].
4. Ellenőrzés és illesztés: a kapott besorolások egyeztetése a fejezet későbbi táblázataiban közölt pontszámokkal és értelmezésekkel; szükség esetén terminológiai finomhangolás a konzisztencia érdekében.

A normatív erő és a technikai lefedettség együttes vizsgálata arra mutat rá, hogy nincs egyetlen, minden dimenzióban ideális dokumentum: a kötelező erejű keretek (pl. típusjóváhagyáshoz kötött előírások) nem feltétlenül biztosítanak teljes technikai mélységet, míg a részletes iparági szabványok nem mindig bírnak közvetlen végrehajthatósággal [61], [62], [66]. A mátrixalapú, súlyozás nélküli értékelés éppen ezért elegendően karcsú a fejezet későbbi számszerű eredményeinek hordozásához, miközben átlátható összehasonlíthatóságot biztosít [65], [68]. A részletes kitöltött mátrix és az összegzett pontszámok a fejezet következő alfejezeteiben találhatók.

2.2.4. Az adatok kódolásának megbízhatósága

A kvalitatív tartalomelemzés egyik alapvető követelménye, hogy a kódolás konzisztens és reprodukálható legyen [69]. A kutatás során ezért alkalmaztam az intercoder agreement módszerét, amely a kódolás megbízhatóságának ellenőrzésére szolgál. Az eljárás lényege,

hogy két független kódoló – jelen esetben a szerző és a kutatásban nem közvetlenül érintett, de a témában jártas szakértő – egymástól függetlenül kódolja ugyanazt az adatanyagot. Az így létrejött kódolási készletek összevetését követően a kódolási eltéréseket közös megbeszélés során oldottuk fel, és konszenzusos kategóriarendszert alakítottunk ki.

Krippendorff [69] hangsúlyozza, hogy az intercoder reliability nem csupán statisztikai mutató, hanem annak biztosítéka, hogy „a kódolási döntések nem önkényesek, és más kutatók is hasonló következtetésekre jutnának azonos adatokból". Az általam alkalmazott módszer e megközelítést követi: a független kódolás és a konszenzusos egyeztetés kombinációja lehetővé tette a kódok jelentésének pontosítását és a kategóriák tartalmi koherenciájának növelését.

Az eljárás egyben illeszkedik [70] által javasolt peer debriefing technikához is, amely a kutatói reflexivitás és az adatelemzés érvényességének növelését célozza. A konzulens bevonása ebben az értelemben kettős szerepet töltött be: egyrészt második kódolóként a megbízhatóságot erősítette, másrészt kritikus szakmai partnerként hozzájárult a kódolási logika finomításához. A kutatásban alkalmazott módszertan egyúttal megfelel az analyst triangulation elvének is, amely több elemző bevonásával biztosítja a megbízhatóságot és elősegíti az alternatív értelmezések feltárását [71]. Ez a megközelítés csökkenti annak kockázatát, hogy a végső kategóriarendszer kizárólag egyetlen kutató szemléletét tükrözze. Továbbá a kutatási folyamatban érvényesült a reflexivity elve is, vagyis a kutató saját szerepének, előfeltevéseinek és értelmezési keretének folyamatos vizsgálata [72]. A reflexív hozzáállás hozzájárult ahhoz, hogy a kódolási döntések és az elemzés során alkalmazott interpretációk átláthatóak és tudatosak maradjanak.

Ezeknek a módszertani elemeknek az együttes alkalmazása biztosítja, hogy a kutatásban kialakított kategóriák és témák nem pusztán egyetlen kutató szubjektív értelmezésén alapulnak, hanem egy független szakmai kontroll és több elemző szempontjának integrált, konszenzusos eredményeként jelennek meg.

2.3. Empirikus kutatás módszertani megközelítése

Az empirikus vizsgálatok célja a járműhasználók adatbiztonsági és adatvédelmi tudatosságának, valamint az iparági szakértők szabályozással és kockázatértékeléssel kapcsolatos tapasztalatainak feltárása. A kutatás során két fő módszertani pillért alkalmaztam: egy kvantitatív kérdőíves adatgyűjtést és egy kvalitatív mélyinterjús

vizsgálatot. Az alábbi alfejezetek részletesen bemutatják e módszerek elméleti megalapozottságát, alkalmazási lépéseit és a kutatás során betöltött funkciójukat.

2.3.1. Kérdőíves adatgyűjtés

A kérdőíves adatgyűjtést a kutatás K3 kérdésének megválaszolására terveztem, amely a felhasználói percepciók és attitűdök vizsgálatára irányul az internetkapcsolattal rendelkező járművek információbiztonságával kapcsolatban. A kvantitatív módszer választását elsősorban az indokolta, hogy nagymintás, statisztikailag elemezhető adatot biztosít, amely lehetővé teszi a felhasználói vélekedések, kockázatészlelés és viselkedési hajlandóság számszerű összehasonlítását különböző demográfiai és használati jellemzők szerint. A kutatás során célzottan a felhasználói tudatosság és informáltság dimenzióira koncentráltam, különösen az adatkezeléshez kapcsolódó biztonsági aspektusokra.

A kérdőíves kutatás módszertani alapját a kvalitatív és kvantitatív elemeket ötvöző, vegyes módszertan (mixed methods megközelítés) képezi [73] [74], [75], [76], [77], 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 fordítottam a kérdésfeltevések egyértelműségére és az elfogultság minimalizálására, hogy a válaszok hitelesen tükrözzék a válaszadók ismeretszintjét és attitűdjeit [78]. 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. A kérdéssor előkészítéshez pilot mintás tesztelést terveztem annak érdekében, hogy a kérdőív végső változata a válaszadók számára érthető, releváns és kellően informatív legyen, és hogy visszajelzést adjon a kérdőív szerkezetéről, logikai felépítéséről és a válaszadók terhelhetőségéről. A pilot fázis alkalmazása a kérdőíves kutatás tervezésének bevett, a társadalomtudományi szakirodalomban széles körben

ajánlott lépése [73]; [79]; [80]; [81]. Az ilyen előzetes tesztelés a szakirodalom szerint különösen indokolt összetett, technológiailag érzékeny témák esetén, mint az internetkapcsolatra képes járművek adatbiztonsága, ahol a fogalmak ismerete és értelmezése a válaszadók körében jelentős eltérést mutathat [82].

A kérdőív szerkesztése során figyelembe vettem a témaspecifikus skálák és kérdéstípusok alkalmazhatóságát. A kérdések között szerepeltek dichotóm, Likert-skálás és nyitott kérdések is, lehetővé téve a válaszadók különböző gondolkodási mintáinak feltérképezését [83]. A validálás során szakértői előtesztet végeztem, amely segített az esetleges félreérthető vagy redundáns kérdések kiszűrésében. A mintavétel nem véletlenszerű, hanem célzott (purposive sampling) stratégiát követett. Az adatfelvétel online kérdőíves platformon keresztül történt, figyelemmel arra, hogy a célpopulációhoz tartozó gépjármű-tulajdonosok könnyen elérhetővé váljanak [84]. A válaszadás önkéntes és anonim módon zajlott.

Bár a kutatás során alkalmazott kérdőíves adatgyűjtés megfelelő módszertani alapokon nyugodott, a kitöltők száma végül a vártnál alacsonyabb maradt, így a minta elemszáma korlátozta a kvantitatív elemzés általánosíthatóságát. A szakirodalomban széles körben elfogadott eljárás, hogy kisebb mintaszám esetén a primer eredményeket összevetik releváns, nemzetközi kontextusban már vizsgált adatokkal és következtetésekkel (pl. [85], [86], így én is ezzel a módszerrel éltem. Ez a módszertani trianguláció, illetve a „comparative contextualization” (összehasonlító kontextualizálás) lehetővé teszi, hogy a kutató saját eredményeit nemzetközi szakirodalmi adatokkal és tapasztalatokkal gazdagítsa, így növelve a kutatás érvényességét és elméleti beágyazottságát [73], [83]. Az összevetés nemcsak az eredmények megbízhatóságát erősíti, hanem lehetőséget teremt arra is, hogy a friss, néhány országra koncentrálódó kutatási tapasztalatokat szélesebb kontextusba helyezve értékeljem, és megvizsgáljam az esetleges hasonlóságokat vagy eltéréseket. Az ilyen összehasonlító elemzés kiemelten ajánlott olyan, empirikus társadalomtudományi kutatásokban, ahol az adatfelvételi korlátok miatt a minta nem tekinthető reprezentatívnak, de a kutatás értékes kvalitatív és komparatív betekintést adhat [73], [83], [84], [85], [86], [87].

Ez a megközelítés lehetővé tette, hogy a kutatás mind módszertani, mind elméleti szempontból illeszkedjen a nemzetközi trendekhez, és a feltárt tapasztalatok relevanciáját a nemzetközi irodalom kontextusában is értelmezni tudjam.

2.3.2. Szakértői mélyinterjúk

A kutatás korábbi, dokumentumelemzésen alapuló szakaszában az autóipari információbiztonsági szabályozások és sztenderdek elméleti és strukturális összefüggéseit vizsgáltam. Ezzel azonban csak részben lehetett választ adni a kutatási kérdésekre, mivel a szabályozások gyakorlati alkalmazása, különösen a kockázatelemzés folyamata, a szervezeti és egyéni döntések élő dinamikájában érthető meg igazán. Ezért a tartalomelemzési munka folytatásaként szakértői mélyinterjúk lefolytatása mellett döntöttem, hogy az elmélet és a gyakorlat közötti szakadékot áthidaljam. A kvalitatív, interjús adatgyűjtés célja az volt, hogy alaposabb, kontextusban gazdagabb megértést nyerjek mind a szabályozási környezet értelmezéséhez (K1), mind a felhasználói tudatosság témaköréhez (K3), de mindenekelőtt a járműipari kockázatelemzési módszerek gyakorlati működésének és korlátainak feltárására (K2) törekedtem.

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 [88]. A 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 megismerjem és összefoglaljam.

Jelen kutatás lefolytatásához ezért a terepkutatás kategóriájába tartozó félig strukturált interjúztatás módszere került kiválasztásra, mint a témához illeszkedő technika [89]. 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 annak feltárása, hogy a jelenleg alkalmazott járműipari kockázatelemzési módszerek mennyiben alkalmasak a valóságban a komplex információbiztonsági kockázatok kezelésére. Cél volt továbbá, hogy a felmerült információbiztonsági problémákkal kapcsolatos megoldási javaslatok is összegyűjtésre kerüljenek. Mivel ez a megközelítés mélyebb dialógust igényel és nem oldható meg például egyszerű kérdőíves módszertannal, ezért indokolt a mélyinterjúk alkalmazása [90]. Az interjú a kérdésfeltevésén és az arra adott válaszok megvitatásán kívül kötetlen formában zajlott,

azaz interaktív beszélgetés keretében, ami megkönnyítette a többletinformációk megszerzését [91].

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.

A kvalitatív kutatás módszertanát félig strukturált mélyinterjúk alkalmazásával valósítottam meg. Ez a technika egy előre megtervezett kérdésvázlatot követ, ugyanakkor teret enged a válaszadók egyéni narratíváinak és szakmai tapasztalatainak [87]. Az interjúk célja a szabályozási környezet értelmezésének gyakorlati aspektusainak feltárása volt. Az interjúk elemzéséhez narratív tartalomelemzést alkalmaztam, amely során nem pusztán a témák azonosítása, hanem azok kontextusba helyezése és az elbeszélések szerkezeti mintázatainak feltérképezése is megtörtént [92]. A módszer lehetővé tette a különböző szakértői nézőpontok integrálását és azok jelentésképző mechanizmusainak vizsgálatát.

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 [69] 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 [69].

A résztvevők kiválasztása célzott, elméleti mintavétel szerint történt (theoretical sampling), figyelemmel a releváns iparági tapasztalatok és szerepkörök reprezentálására. Az interjúkat rögzítettem, majd szó szerinti átiratot készítettem. A kódolás induktív megközelítéssel zajlott, nyílt és tematikus kódolási szinteken keresztül [93].

2.4. Kommunikációs protokollok biztonsági modellezésének módszertani alapjai

Az internetkapcsolattal rendelkező járművek adatkommunikációs rendszerének biztonsági vizsgálatához olyan módszertani keretet alakítok ki, amely egységesen képes értékelni az alkalmazott protokollok biztonsági szintjét, a lehetséges rejtett adatcsatornákat, valamint az adatvédelmi kockázatokat. A kutatás kiindulópontját az adja, hogy a K4 kutatási kérdés megválaszolásához nemcsak a hagyományos támadási felületeket, hanem a protokollok rejtett információtovábbítási lehetőségeit is átfogóan szükséges értékelni [94], [95], [96].

Első lépésként a kommunikációs protokollok biztonsági elemzését az OSI modell rétegei mentén tervezem elvégezni, amely lehetővé teszi az egyes adatátviteli megoldások strukturált és összehasonlítható vizsgálatát [97], [98]. Ebben a fázisban az üzenettípusok, fejlécmezők, titkosítási lehetőségek és hitelesítési mechanizmusok rendszerezett feltárására törekszem. Az aktuális szakirodalom alapján kiemelt figyelmet fordítok a könnyűsúlyú, IoT-környezetben is alkalmazott protokollok sajátosságaira, hiszen ezek a modern járművekben is egyre elterjedtebbek [94], [95], [98].

A protokollrétegek áttekintését követően a fenyegetések és kockázatok modellezésére a STRIDE módszertant alkalmazom, amely átfogóan képes feltérképezni a klasszikus támadási vektorokat, valamint az autóiparban kiemelten fontos jogosultság-kezelési, naplózási és információszivárgási kérdéseket is [99]. Az elemzés során azonban nem csupán a hagyományos STRIDE kategóriákra szorítkozom, hanem kiegészítem a vizsgálatot a rejtett csatornák (covert channels) detektálhatóságával és kihasználhatóságával is, támaszkodva a legújabb, 2022 utáni szakirodalmi eredményekre [96], [97], [98]. Ezzel biztosítom, hogy a vizsgálat nemcsak a jól ismert támadási lehetőségeket, hanem a kevésbé nyilvánvaló, metaadatokon vagy időzítésen alapuló információelrejtési technikákat is lefedje.

A harmadik pillérként az adatvédelmi (privacy) szempontokat integrálom az elemzési keretbe. Külön figyelmet fordítok a titkosítási megoldásokra, a hozzáférés-vezérlésre, valamint azokra a kriptográfiai algoritmusokra, amelyek a személyes adatok védelmét hivatottak biztosítani – különösen a korlátozott erőforrású eszközöket is figyelembe véve [98], [100].

Az összefoglalt módszertani megközelítés célja, hogy a protokollok biztonsági vizsgálata strukturált, rétegezett elemzésen, fenyegetésmodellezésen és adatvédelmi szempontrendszeren alapuljon. Ez lehetővé teszi, hogy átfogó képet kapjak a modern internetkapcsolatra képes járművek kommunikációs rendszerének biztonsági és adatvédelmi kihívásairól, és a konkrét elemzések során a megfelelő értékelési szempontok mentén vizsgáljam a leggyakrabban használt technológiákat.

2.5. Az adattovábbítás mennyiségi modellezésének módszertani alapjai

A kutatás ötödik kérdése, miszerint „Milyen módon használhatók fel az internetkapcsolattal rendelkező járművek szenzor- és kommunikációs adatai kijelölt objektumok vagy célszemélyek rejtett megfigyelésére, és ez milyen nemzetbiztonsági kockázatokat hordoz flottaszinten?”, olyan módszertani megközelítést igényelt, amely képes a járművek mozgásából és adatküldési képességéből származó lefedettségi és megfigyelési potenciál számszerű megbecslésére. A vizsgálat során két, a szakirodalomban széles körben alkalmazott módszertani keretet vettem alapul, bár a gyakorlatban ezek adaptált formában jelentek meg.

Az elemzés célja, hogy bemutassa, az internetkapcsolattal rendelkező járművek által generált és továbbított szenzoradatok — különösen a képi, hang- és geolokációs információk — milyen módon használhatók fel rejtett megfigyelésre, illetve ezek továbbítása milyen kockázatot hordoz flottaszinten. A modellezési és elemzési lépések módszertani megalapozását az alábbiak szerint építettem fel:

2.5.1. Rejtett csatornás adattovábbítás – elméleti lehetőségek

A kutatás első lépéseként azt vizsgálom, hogy a kommunikációs protokollok — különösen az alkalmazásrétegi (pl. MQTT, CoAP) és transzport/hálózati rétegű protokollok — milyen technikai lehetőségeket kínálnak a képi, hang- vagy helyadatok rejtett továbbítására. A módszertan támaszkodik a klasszikus információ-elrejtési és szteganográfiai taxonómiákra, különös tekintettel a Zander és munkatársai által felvázolt

elméleti keretre, amely az információrejtést storage és timing csatornák szerint csoportosítja [101], valamint a Velinov és munkatársai. által végzett MQTT-rejtett csatornavizsgálatokra [102]. Az elemzés során áttekintem, hogy az egyes adatkategóriák (kép, hang, geolokáció) milyen szteganográfiai megoldásokkal és protokollmezőkben (pl. payload, topic, fejléc) juttathatók el rejtett módon, mind elméleti, mind kísérleti demonstrációk alapján.

Az első lépésben a gépjárművek fedélzeti kamerái által rögzített képadatok továbbításának lehetőségeit vizsgálom, a szenzoradatok adattípusait, felbontását, tömörítési eljárásait (pl. JPEG, H.264), és azt, hogy ezek a képi információk mennyire alkalmasak arcfelismerésre, rendszámfelismerésre, illetve egyéb személyes információk kinyerésére. A módszertan itt a számítógépes látás és adatvédelmi szakirodalom standard eljárásait követi (lásd pl. a Molnár–Csábrági–Forstner-kategorizációt [103]), kiegészítve a fedélzeti rendszerek képrögzítési és továbbítási kapacitásainak leírásával. Kiemelten szerepel a képadatokból automatizáltan kinyerhető, személyhez köthető információk kockázatelemzése.

A második módszertani pillér a fedélzeti mikrofonok vagy infotainment rendszerek által generált hangadatok vizsgálata. Itt a fókusz az adatok rögzítésének minőségén, a tömörítési (pl. MP3, AAC) és továbbítási lehetőségeken, valamint a beszédfelismerési/azonosítási kockázatokon van. Elemzem, hogy milyen szinten lehet visszafejteni vagy azonosítani személyeket, és hogy a hangadatok mennyiben járulnak hozzá a megfigyelési potenciál növeléséhez. A szakirodalmi alapot részben a speech-to-text és biometrikus azonosítás területén elért eredmények adják [104].

A harmadik vizsgálati lépésben a GPS, illetve egyéb helymeghatározási adatok adatvédelmi és biztonsági szempontú elemzése történik.

2.5.2. Elméleti modell kialakítása – az okosjárművekkel végzett megfigyelésben rejlő potenciál

Az első módszertani alap a mobil szenzorhálózatok lefedettségi modellje. Ebben a megközelítésben a kompromittált járművek funkcionálisan mozgó szenzorcsomópontokként értelmezhetők, amelyek a célterület – például egy épület – környezetének folyamatos vagy részleges lefedésére irányulnak. A lefedettség számításához a szakirodalom geometriai és valószínűségi modelleket javasol, például Poisson-folyamatokat és véletlenszerű mozgásmodelleket (random waypoint) [105],

[106]. Ezek segítségével becsülhető, hogy adott számú és mozgásmintázatú jármű milyen valószínűséggel és gyakorisággal képes megfigyelni a célpontot. A modell előnye, hogy skálázható, így flottaszinten is képes megbízható becslést adni a potenciális megfigyelési kapacitásról.

A második módszertani pillért a forgalmi és megfigyelési szcenárió-szimuláció képezte. Ez a megközelítés valós vagy szimulált forgalmi adatokra épít, és azt vizsgálja, hogy a járművek mozgási mintázata és adatküldési gyakorisága miként befolyásolja a célpont megfigyelésének gyakoriságát és időbeli eloszlását. Hasonló megközelítést korábbi kutatásokban buszokra alapozott mobil szenzorhálózatok esetében is alkalmaztak, ahol a lefedettség az útvonalak mentén értelmeződött [107]. A módszer előnye, hogy közvetlen kapcsolatban áll a kutatás során alkalmazott, járműszám és képkészítési gyakoriság összefüggését bemutató modell eredményeivel.

A jelen kutatásban e két módszertani keret adaptált kombinációját alkalmaztam. Noha a szakirodalomban rögzített formájukban ezek a modellek komplexebb adatigényt és formálisabb validációs lépéseket kívánnának, a dolgozatban bemutatott elméleti modell, amely egy Budapest méretű város forgalmas részén elhelyezkedő célobjektum teljes vagy részleges megfigyeléséhez szükséges járműszámot és adatküldési rátát becsüli, mivel nem valós helyzetből indul ki, elegendő pontossággal bír és a nemzetbiztonsági kockázatok bemutatása szempontjából releváns eredményeket nyújt. A módszertan alkalmasságát alátámasztják a mobil szenzorhálózati és járműalapú megfigyelési rendszerekről szóló nemzetközi kutatások is, amelyek bizonyították, hogy viszonylag korlátozott számú mozgó egység is képes jelentős területi lefedettséget biztosítani [108].

3. AZ AUTÓIPARRA VONATKOZÓ SZABÁLYOZÁSI KÖRNYEZET TARTALOMELEMZÉSE ÉS FUNKCIONÁLIS VIZSGÁLATA

A kutatási szakasz célja annak vizsgálata volt, hogy az Európai Unió jelenlegi szabályozási keretrendszere milyen mértékben képes védelmet nyújtani az internetkapcsolattal rendelkező személygépjárművekkel szemben fennálló információbiztonsági fenyegetésekkel szemben. A K1 és K2 kutatási kérdések megalapozták az elemzés irányát és struktúráját. A negyedik ipari forradalom technológiai áttörései a társadalmi és gazdasági rendszereket szoros kapcsolatba hozták a digitális infrastruktúrákkal. Az IoT-eszközök tömeges elterjedése új sebezhetőségeket hozott létre: a 2016-os Mirai botnet-támadás több százezer IP-alapú eszköz bevonásával

bénította meg a globális internetforgalmat [109]. Az incidens rávilágított, hogy a fizikai védelemre épülő megközelítést átfogó kockázatmenedzsmenttel kell felváltani, amely a szoftveres és hálózati biztonságot is magában foglalja. A Vault 7-ből kiszivárgott CIA-dokumentumok pedig azt mutatták, hogy állami szereplők is képesek kihasználni az okoseszközök sebezhetőségeit [109]. Az európai kiberbiztonsági szabályozás az elmúlt évtizedben erősödött, különösen a közös normák és koordinált technológiai válaszok kialakításában. A 2019/881-es Cybersecurity Act mérföldkőnek számít, mivel megerősítette az ENISA mandátumát és egységes keretet teremtett a kibervédelmi tanúsításhoz [109]. Célja az uniós együttműködés, az ellenállóképesség és a bizalom növelése. A 2021–2027-es pénzügyi keret kiemelten támogatja az AI- és Big Data-alapú fenyegetésészlelést, prediktív elemzést és incidenskezelést, elősegítve az innováció és biztonság együttes fejlődését. Az ipar, a tudomány és a kormányzat együttműködése kulcsfontosságú az európai technológiai autonómia megerősítésében az amerikai és kínai befolyással szemben.

Az elmúlt évek jelentős előrelépésének tekinthető a TISAX (Trusted Information Security Assessment Exchange)[3]és az ISO/SAE 21434[4] megjelenése, melyek specifikusan a személygépjárműipar igényeire szabott információbiztonsági szabványok. Az ISO/SAE 21434 egy termékközpontú autóipari szabvány, amely meghatározza a közúti járművek elektromos és elektronikus (E/E) rendszereinek – alkatrészeik és kapcsolódási pontjaik – kiberbiztonsági kockázatkezelési követelményeit a koncepciótól a leszerelésig. A dokumentum egységes keretrendszert biztosít a kiberbiztonsági folyamatok és a kockázatkommunikáció számára, igazodva a nemzetközi információbiztonsági trendekhez. Bár ígéretes, a 2021-ben kiadott szabvány alkalmazása nem kötelező, és piaci elterjedése időigényes. A TISAX egy autóipari értékelési keretrendszer, amely az ISO/IEC 27001-re épül, de kifejezetten a beszállítók biztonsági kockázatainak kezelésére készült. Célja az egységes, független értékelés és a biztonsági szintek összehasonlíthatósága. A rendszer előnyös a beszállítóknak is, mert bizonyíthatják megfelelőségüket, és támogatást kapnak saját biztonsági folyamataik fejlesztéséhez [110]. Ezt a szabályozási törekvést egészítik ki az ENSZ EGB (vagyis nemzetközi nevén UNECE) WP.29 R155 és R156 rendeletei, amelyek 2022 júliusától kötelezőek az új

[3] TÜV SÜD: TISAX. URL: https://www.tuvsud.com/en/services/auditing-and-system-certification/tisax (letöltve: 2025.08.10)
[4]ISO: ISO/SAE 21434. URL: https://www.iso.org/standard/70918.html (letöltve: 2025.08.10)

típusjóváhagyásokhoz, és előírják a járművek kiberbiztonsági menedzsmentrendszerének, valamint szoftverfrissítési képességeinek meglétét és megfelelőségét is.[5] Európai uniós szinten a Cyber Resilience Act (CRA)[6] célja tovább szigorítani az intelligens járművek és beszállítói rendszerek kiberbiztonsági követelményeit, amely horizontális szabályozásként minden digitális elemet tartalmazó termékre érvényes lesz – beleértve a járműipari szoftvereket és hardvereket is.

A fenti szabványokon kívül érdemes még említést tenni az IEC 62443-ról[7], mely kifejezetten az ipari ellenőrzési rendszerekre vonatkozik, illetve a SAE J3061[8] 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). 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 alkalmazhatják (például ISO/TS 16949, amely az általános, ISO 9001 minőségbiztosítási szabvány autóipari leképezése), amelyek lehetnek nemzetközi vagy helyi szintűek.

Az Európai Unióban a személygépjárművekre vonatkozó kötelező előírásokat az Európai Bizottság dolgozza ki, míg a részletes technikai szabványokat nemzetközi szervezetek (UNECE, ISO, CEN) határozzák meg. Az Egyesült Államokban a szabályozásért a NHTSA felel, a részletes követelményeket pedig független szakmai szervezetek alakítják, így a gyakorlat jelentősen eltérhet az európaitól. A dolgozat középpontjában az uniós szabályozás áll, de az amerikai rendszer érintőleges bemutatása indokolt, mivel a globális autógyártók és beszállítók transzatlanti jelenléte miatt a két piac kölcsönösen hat egymásra. Az EU-ban az elmúlt években a GDPR kiemelt szerepet kapott, és ennek

---

[5] United Nations Economic Commission for Europe, *UN Regulation No. 155 and No. 156 (WP.29)*. URL:https://unece.org/transport/vehicle-regulations (letöltve: 2025.08.10)

[6] European Commission, *Proposal for a Regulation on horizontal cybersecurity requirements for products with digital elements (Cyber Resilience Act)*. URL:, https://digital-strategy.ec.europa.eu/en/policies/cyber-resilience-act (letöltve: 2025.08.10)

[7] ISA: ISO 62443. URL: https://www.isa.org/standards-and-publications/isa-standards/isa-iec-62443-series-of-standards (letöltve: 2025.08.10)

[8] SAE: J3061. URL: https://www.sae.org/standards/content/j3061_201601 (letöltve: 2025.08.10)

hatására az adatvédelem más szabványokban is egyre hangsúlyosabbá vált. Ugyanakkor a fogyasztói adatok és az adatáramlás átláthatósága kizárólag a GDPR közvetlen fókusza. Bár a rendelet teljes körű elemzése nem célja e munkának, a nemzetközi szakirodalom alapján egyértelmű, hogy fejlesztésre szorul [111], [112], [113]. 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
- CRA – Cyber Resilience Act
- 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

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

Az előző fejezetekben bemutatott jogszabályok és szabványok jól kiegészítik egymást: egyesek funkcionális, mások adatvédelmi vagy fenyegetésalapú megközelítést alkalmaznak. Ugyanakkor érvényesítésük ritkán történik egységesen, mivel többségük nem kötelező, és felügyeletükre nincs kijelölt hatóság.

Bár az UNECE R155 és R156 rendeletek, valamint a Cyber Resilience Act (CRA) fontos lépést jelentenek az egységesítés felé, a szabályozási környezet továbbra is széttöredezett. A járművek, mint hálózatba kapcsolt rendszerek, egyszerre több, gyakran átfedő szabvány hatálya alá tartoznak. Ezek eltérő aspektusokat fednek le – a szervezeti működéstől a szoftverfrissítési folyamatokig –, így a követelmények között hiányosságok, átfedések és akár ellentmondások is előfordulnak.

Egységes iránymutatás jelenleg nem létezik arra, hogy e szabályok miként viszonyulnak egymáshoz. Tovább nehezíti az értelmezést, hogy az R155–R156 gyakran más szabványokra, például az ISO/SAE 21434-re vagy az ISO/IEC 27001-re épül, ami bár elősegíti az összehangolást, egyben növeli a megfelelés komplexitását a gyártók és beszállítók számára.

Az eddigiekben említett, főbb járműipari kiber- és információbiztonsági előírásokat jogi kötelező erejük, alkalmazási körük, felügyeleti mechanizmusuk és szankciórendszerük szerint is megvizsgáltam – a részletes elemzést a 3. Számú mellékletben szereplő táblázat foglalja össze. Az összehasonlítás alapján a járműipari kiberbiztonsági szabályozás továbbra is széttöredezett és részleges, gyakran párhuzamos vagy átfedő követelményeket tartalmaz. Egyes előírások iparági szabványok (pl. ISO/SAE 21434, ISO/IEC 27001, TISAX), míg mások kötelező rendeletek (pl. UNECE R155–R156, CRA, GDPR), ám lefedettségük és fókuszuk eltérő. A legtöbb szabvány a szervezeti működésre vagy a technikai komponensekre koncentrál, így a jármű mint egységes informatikai rendszer átfogó kezelése továbbra is hiányzik. További nehézséget okoz, hogy több szabályozás egymásra épül (pl. az R155 az ISO/SAE 21434 alapelveit alkalmazza), ami bonyolítja a megfelelést és az értelmezést. A tanúsítási és auditálási gyakorlatok szigora pedig attól függően változik, hogy az adott követelmény jogi vagy piaci alapú.

3.3. A keretalapú tartalomelemzés (Framework Analysis) eredményei

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.

A 4. Számú mellékletben a járműipari szabványokat és jogszabályokat tematikus kategóriák szerint rendszereztem, bemutatva fő céljaikat, alkalmazási területeiket és kulcskövetelményeiket. Az indexelés célja, hogy átlátható képet adjon a szabályozási környezet struktúrájáról, és láthatóvá tegye az egyes előírások közötti kapcsolódásokat, átfedéseket és eltéréseket. A módszer nem a szabályozások teljes körű elemzésére, hanem a személygépjárművek integrált információbiztonsági megközelítése szempontjából releváns elemek kiemelésére szolgál. Az előírások összevetése alapján a kiber- és információbiztonsági követelmények hangsúlyosan jelen vannak, de a szabványok fókusza eltér: míg az ASPICE és az AUTOSAR Adaptive Platform a szoftverfejlesztés strukturáltságát célozza, addig a GDPR és a TISAX az adatkezelés és ellátási lánc biztonságát erősíti.

A K1 és K2 kutatási kérdésekhez kapcsolódva megállapítható, hogy e szabványok elemei nem biztosítanak egységes, átlátható védelmet sem a jármű, sem a gyártó szintjén, különösen az internetkapcsolattal rendelkező járművek esetében. A legtöbb előírás technikai vagy szervezeti fókuszú, és hiányzik közülük az a komplex megközelítés, amely az autóipari ökoszisztémát egészként kezeli.

A további elemzés ezért azokra a szabványokra koncentrál, amelyek közvetlenül kapcsolódnak a személygépjárművek szabályozási hiányosságaihoz és a kockázatelemzési módszerek korlátaihoz. A jelenlegi előírások csak részben foglalkoznak az adatok megosztásának és kezelésének feltételeivel, ami további kutatást igényel.

Elméleti szinten a kiberbiztonsági (pl. ISO/SAE 21434, UNECE R155–R156), információbiztonsági (pl. ISO/IEC 27001, GDPR) és funkcionális biztonsági (pl. ISO 26262, ISO 21448) szabványok integrációja szinergikus hatást eredményezhet, különösen az AUTOSAR, ASPICE, CISPR 25 és ISO 24089 kiegészítő szerepével. A gyakorlatban azonban e szabványok egyidejű és konzisztens alkalmazása ritka, mivel a megfelelés jelentős erőforrásokat igényel és gyakran átfedésekkel jár. Ez is alátámasztja egy átlátható, harmonizált szabályozási keretrendszer szükségességét.

3.4. A tematikus elemzés (Thematic Analysis) eredményei

Az első lépés során részletesen áttekintettem az egyes szabványokat és jogszabályokat, azonosítva fő célkitűzéseiket, strukturális jellemzőiket és azt, hogy mely alkalmazási területeken nyújtanak iránymutatást. Ez az átfogó áttekintés alapot teremtett annak megértésére, hogy ezek az előírások milyen mértékben és milyen megközelítésben kapcsolódnak az autóipari információbiztonság és kiberbiztonság problématerületeihez. A tematikus elemzés eredményei egyben irányt mutattak a keretelvű (framework) elemzés számára is: a feltárt témák és összefüggések segítettek kijelölni azokat a kulcsterületeket és szempontokat, amelyek mentén a szabályozási dokumentumok tartalma strukturáltan összehasonlíthatóvá vált. Ennek eredményeképpen a framework analysis során már előre meghatározott, releváns dimenziók mentén vizsgálhattam a szabványok közötti eltéréseket, átfedéseket és hiányosságokat, tovább gazdagítva a szabályozási környezet kritikai értékelését.

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).

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

- Kiberbiztonsági védelmi rendszerek és eljárások: Számos szabvány (pl. ISO/SAE 21434, SAE J3061, UNECE WP.29 R155, valamint a CRA) központi eleme a fenyegetésmodellezés, a kockázatelemzés és az incidenskezelés. A CRA horizontális, eszközfókuszú megközelítése révén a termék- és beágyazott rendszerszintű kiberbiztonságot is szabályozza.
- 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.

A témakörök újraértékelése során megerősítést nyert, hogy bizonyos szabványok több tematikai egységgel is átfedést mutatnak. Ilyenek például a kiberbiztonság és adatvédelem határterületei (pl. CRA, GDPR), illetve a funkcionális biztonság és a frissítési eljárások összekapcsolódása (pl. ISO 26262 és ISO 24089). Ez az átfedés jól tükrözi a személygépjárművek technológiai összetettségét, valamint a szabályozási keretek közötti integrációs kihívásokat.

A témák áttekintése után a következő elnevezésekkel határoztam meg őket:

- Kiberbiztonság és fenyegetéskezelés: A járműrendszerek védelmét célzó előírások, amelyek a kockázatelemzésre, támadási vektorok azonosítására és a megelőző intézkedésekre fókuszálnak (pl. ISO/SAE 21434, CRA, R155).
- 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.

A tematikus elemzés megerősítette, hogy az autóipari szabványok és szabályozások több, egymással részben átfedő biztonsági célterületet fednek le. Az ISO/SAE 21434, az UNECE R155-R156 és a Cyber Resilience Act különösen fontos szerepet játszanak a járművek kiberbiztonsági megfelelőségének kialakításában. A CRA horizontális jellegénél fogva túlmutat a klasszikus autóipari szabályozásokon, mivel az intelligens és hálózatba kapcsolt termékek, köztük a járművek beépített digitális elemeire is kiterjed. A GDPR és a TISAX továbbra is kiemelt jelentőségűek a személyes és szervezeti adatok védelmében, különösen az ellátási lánc összetett adatáramlási folyamataiban. A funkcionális biztonság terén az ISO 26262 és ISO 24089, valamint az ezek alapján készült R156 biztosítják a jármű működésének integritását és a szoftverfrissítések biztonságos menedzselését. A szoftverfejlesztés területén az AUTOSAR és ASPICE keretek támogatják a magas szintű rendszerintegrációt, míg a CISPR 25 révén az elektromos rendszerek zavartűrése válik biztosíthatóvá. Mindezek alapján a K1 és K2 kérdésekkel kapcsolatban megerősítést nyer az az állítás, hogy a jelenlegi szabályozási környezet bár sokrétű, nem képes teljes mértékben és egységesen kezelni az internetkapcsolattal rendelkező személygépjárművekkel szembeni komplex kockázatokat sem a termék, sem a szervezeti oldalról.

3.5. Szabványok vizsgálata funkcionális összehasonlítás alapján

A személygépjárművekre vonatkozó szabványok értelmezéséhez elengedhetetlen a funkcióalapú és életciklus-szemléletű megközelítés, mivel a jármű biztonságát a teljes élettartam – a koncepciótól a bontásig – befolyásolja. Az elemzés során a szabályozások

tartalmi és jogi természetét is értékeltem, különválasztva a soft law (ajánlások, iparági sztenderdek) és hard law (kötelező jogszabályok) elemeket, amelyek meghatározzák a gyakorlati végrehajtás mélységét és a védelmi szintet.

Az életciklus-orientált megközelítés rávilágít arra, hogy az egyes fázisokban (pl. vásárlás, használat, továbbértékesítés, bontás) eltérő fenyegetések és felelősségi kérdések jelennek meg – különösen az adattárolók és szenzoradatok kezelésével kapcsolatban. A vizsgálat célja az volt, hogy feltárja, a különböző szabályozások milyen mértékben járulnak hozzá a jármű biztonságos működéséhez, és hogyan reagálnak az életciklus során felmerülő kockázatokra.

A kvalitatív tartalomelemzés során az előírások strukturált és összehasonlítható elemeit azonosítottam [3], majd ezek alapján súlyozásos értékelést (Simple Additive Weighting, SAW) végeztem, amely a szabványok lefedettségét és gyakorlati jelentőségét számszerűsítve hasonlította össze. Az elemzés figyelembe vette, hogy az egyes támadástípusok mely járműrendszereket (pl. firmware, szenzorok, kommunikációs buszok, tárolt adatok) érintik, és ezek védelmét a különböző szabványok milyen szinten biztosítják.

Az életciklus-alapú fenyegetéselemzés alapján (részletek az 5. Számú mellékletben) a különböző életciklus-szakaszok eltérő védekezési mechanizmusokat igényelnek, ezért egyetlen szabvány sem képes önállóan lefedni minden kockázati szcenáriót. Indokolt tehát a többféle szabvány együttes, összehangolt alkalmazása, különösen a korábban feltárt szabályozási és kockázatelemzési hiányosságok fényében. A támadástípusok elemzése során figyelembe vettem, hogy azok mely járműrendszer-elemeket (pl. firmware, kommunikációs buszok, szenzorok, tárolt adatok) érinthetik, illetve milyen mértékben képesek az egyes szabványok e részegységek védelmét biztosítani.

A járműipari kiberbiztonsági fenyegetések vizsgálata során szükségessé vált annak feltérképezése, hogy a különböző típusú támadások mely technikai komponenseket érintik leginkább. A támadási módszerek és célfelületek szisztematikus rendszerezése elősegíti annak megértését, hogy a járművek mely pontjai igényelnek fokozott védelmet, és milyen jellegű biztonsági intézkedésekre van szükség a megelőzés és a detektálás szintjén. A 9. táblázat a támadástípusokat vetíti rá a leggyakrabban célzott technológiai elemekre.

Támadás neve	Távoli hozzáférés	Tárolt adatok	Szenzor	CAN	Firmware	Supply chain	Privát adatok
OBD-II port manipuláció		✓		✓			
CAN-busz injekció				✓			
Keyless entry visszajátszás	✓		✓				
Bluetooth/Wi-Fi sebezhetőségek	✓						✓
Infotainment rendszer kihasználása	✓				✓		✓
OTA frissítések manipulálása	✓				✓		
Telematikai adatok kiszivárgása		✓					✓
Felhasználói eszközök támadása		✓					✓
Töltőállomás manipulálása	✓				✓		
Akkumulátor-kezelő rendszer támadása			✓		✓		
Ransomware (vállalati rendszerek)		✓				✓	
Beszállítói rendszerek kompromittálása		✓				✓	✓

1. *táblázat - Kibertámadási technikák és azok célfelületei személygépjárművek esetében. Forrás: saját forrás.*

A fenti táblázat szemlélteti, hogy az internetkapcsolattal rendelkező személygépjárművek milyen sokféle támadási felületet kínálnak, és ezek milyen típusú támadásokhoz kapcsolódnak. Különösen kiemelkedik a távoli hozzáférési lehetőségek szerepe, amely a legtöbb modern fenyegetési forma közös nevezője (pl. keyless entry visszajátszás, infotainment rendszer kihasználása, OTA manipuláció). A CAN-busz és a firmware sebezhetőségei a jármű belső kommunikációs és vezérlőrendszereinek gyenge pontjaira világítanak rá, míg a tárolt adatok és a privát információk kompromittálása az adatvédelem és az utólagos felelősség kérdéseit is felveti – különösen a GDPR és a CRA értelmében.

A supply chain és a beszállítói rendszerek elleni támadások rávilágítanak az iparági együttműködés sebezhetőségére és arra, hogy egyes támadástípusok – például a

ransomware vagy az OTA-manipuláció – egyszerre több technológiai réteget is érintenek. Ez interdiszciplináris védekezési stratégiákat és egységes szabályozási szemléletet igényel.

A továbbiakban még részletesebben elemeztem a szabályozási környezetet és nemcsak a konkrét fenyegetések feltérképezésére összpontosítottam, hanem arra a kérdésre is választ kerestem, hogy a jelenlegi szabályozások – különösen az ISO/SAE 21434, az UNECE R155, valamint a Cyber Resilience Act (CRA) – milyen mértékben képesek lefedni ezeket a kihívásokat. Ehhez az elemzéshez a módszertani fejezetben bemutatott SAW-módszertanon alapuló szempontrendszert használtam, önálló értékelési rendszer kidolgozásával. (Részletek a 6. számú mellékletben).

Az elemzéshez mátrixalapú értékelési modellt alkalmaztam, amely két fő dimenzió mentén vizsgálta a szabványokat: egyrészt a normatív megfelelőség szempontjából, vagyis a jogszabályi kötelező erő, a hatósági felügyelet és a szankcionálhatóság mértéke szerint; másrészt a technikai lefedettség alapján, amely a nyolc leggyakoribb támadási célpont – például a távoli hozzáférési csatornák, a szoftver- és hardverkomponensek, a beszállítói lánc, valamint a felhasználói adatok – védelmére való alkalmasságot értékelte. A súlyozott értékelést a Simple Additive Weighting (SAW) módszerrel végeztem, amely lehetővé tette a kvalitatív és kvantitatív szempontok összevetését. A modell a szabványok komplexitását és gyakorlati alkalmazhatóságát egyaránt értékelte. Az összesített eredmények alapján az UNECE R155–R156 bizonyult a leghatékonyabbnak (13 pont), ezt követte a CRA (11 pont) és az ISO/SAE 21434 (9 pont). Közepes védelmi szintet ért el az ISO/IEC 27001 és a NIST Cybersecurity Framework (8–8 pont), míg az ISO 26262 mindössze 4 ponttal „nem megfelelő” besorolást kapott. Az eredmények azt mutatják, hogy bár az R155–R156 rendeletek jelentős előrelépést jelentenek, még nem biztosítanak teljes körű védelmet minden területen. Különösen az ellátási lánc biztonsága és a szenzorokkal kapcsolatos fenyegetések kezelésében tapasztalhatók hiányosságok, ami további szabályozási és technológiai fejlesztéseket tesz szükségessé.

3.5.1. Az UNECE R155 és R156 szabályozások szerepe és korlátai az Európai Unió járműipari információbiztonságban

Az Európai Unióban az R155 és R156 szabályozások bevezetése jelentős lépést jelentett a járműbiztonság terén, mivel ezek az első kötelező érvényű előírások, amelyek célja a járművek és a kapcsolódó rendszerek biztonságának biztosítása. E szabályozások előírják

a gyártók számára a Kiberbiztonsági Menedzsment Rendszer (CSMS) és a Szoftverfrissítési Menedzsment Rendszer (SUMS) bevezetését és fenntartását. Ugyanakkor, a gyakorlati alkalmazás során számos kihívás és hiányosság merült fel, amelyek kérdéseket vetnek fel a szabályozások hatékonyságával kapcsolatban.

Bár az R155 elvárja valamilyen menedzsment keretrendszer bevezetését, nem nyújt útmutatást a megvalósításhoz, hanem más szabványnak vagy jogszabálynak (jellemzően az ISO21434-nek) való megfeleléssel javasolja ezt megoldani. Ez különösen problémás lehet a kisebb gyártók számára, akiknek nincs elegendő erőforrásuk további szabványoknak való megfelelésre, nem beszélve a saját megoldások kidolgozásáról [114].

Az R155 és R156 szabályozások csak az új járműtípusokra vonatkoznak, és nem terjednek ki a már forgalomban lévő járművekre. Ez azt jelenti, hogy a meglévő járműflották, amelyek potenciálisan sebezhetőek lehetnek, nem esnek a szabályozás hatálya alá, így továbbra is kockázatot jelenthetnek a közlekedésbiztonságra és az adatvédelemre [115]. A szabályozások végrehajtásához szükséges auditálási folyamatokhoz megfelelő számú és képzett auditorcégre van szükség. Jelenleg azonban nincs elegendő auditorcég, és nem létezik egységes, hivatalos auditmódszertan. Ez azt eredményezi, hogy az auditok minősége és mélysége jelentősen eltérhet, ami aláássa a szabályozások egységes alkalmazását és hatékonyságát [116].

A két rendelet ugyan előírja a gyártók számára a kiberbiztonsági menedzsment rendszerek bevezetését, nem határozzák meg egyértelműen a beszállítók felelősségi körét és a megfelelőség ellenőrzésének módját. Ez nehézségeket okoz a teljes beszállítói lánc ellenőrzésének biztosításában, mivel a beszállítók nem kötelesek közvetlenül megfelelni a szabályozásoknak, még akkor sem, ha termékeik jelentős kockázatot jelentenek, de az sem elvárható, hogy kiadják a megrendelő szervezeteknek az összes olyan érzékeny adatot, amelyek alapján ők elvégezhetnék a megfelelőséghez szükséges vizsgálatokat [117]. A szabályozások elvárják, hogy a gyártók a járművek teljes életciklusa alatt biztosítsák a kiberbiztonsági támogatást és frissítéseket. Azonban nem nyújtanak útmutatást arra vonatkozóan, hogyan kezeljék a technológiai elavulást és a hosszú távú támogatás kihívásait, sőt, egyes esetekben ellentmondásba kerülnek más szabványokkal, adatmegőrzési elvárásokkal. Az elavulásra vonatkozó követelmények különösen problémásak lehetnek, mivel a járművek hosszú élettartama miatt a gyártóknak

biztosítaniuk kell a szoftveres frissítéseket és támogatást hosszú időn keresztül, ami jelentős erőforrásokat igényel [118]. Ugyanehhez a problémakörhöz sorolható (ellentmondásossága miatt) az a tény, hogy a rendeletek érintik a járművek és a felhasználói adatok védelmét, nem biztosítanak közvetlen összhangot az adatvédelmi szabályozásokkal, mint például a GDPR. Ez jogi és megfelelőségi kihívásokat eredményezhet, különösen az adatkezelés és -tárolás terén, mivel a gyártóknak egyszerre kell megfelelniük a biztonsági és adatvédelmi előírásoknak [119].

Összegzésképpen elmondható, hogy az R155 és R156 szabályozások bevezetése fontos lépést jelentett a járműbiztonság terén az Európai Unióban. Ugyanakkor, a gyakorlati alkalmazás során számos kihívás és hiányosság merült fel, amelyek kérdéseket vetnek fel a szabályozások hatékonyságával kapcsolatban. A technikai útmutatás hiánya, a korlátozott hatókör, az auditorcégek és auditmódszertan hiánya, a beszállítói lánc kihívásai, az életciklus-kezelés és támogatás problémái, valamint az adatvédelmi szabályozásokkal való összhang hiánya mind olyan területek, amelyek további fejlesztést és szabályozást igényelnek.

3.5.2. A Cyber Resilience Act (CRA) szerepe és korlátai a járműipari információbiztonságban

Az Európai Unió Cyber Resilience Actje (CRA), amelyet 2024-ben fogadtak el, egységes kiberbiztonsági követelményrendszert hoz létre minden hálózatra kapcsolt termék – így az okosjárművek – számára [120]. A rendelet célja, hogy a gyártók a fejlesztés teljes életciklusa során alkalmazzák a security-by-design elvet, kockázatalapú megközelítést kövessenek, biztosítsák a sebezhetőségek kezelését, és működjenek együtt a piacfelügyeleti hatóságokkal [121]. A CRA hatálya kiterjed minden olyan járműipari komponensre, amely adatátvitelre képes, például infotainment-rendszerekre, OTA-frissítési modulokra és szenzorhálózatokra. Az előírások kötelező érvényűek az EU egész területén, és elméletileg összhangban állnak az UNECE R155–R156 és az ISO/SAE 21434 célkitűzéseivel, azonban a CRA jogilag is kikényszeríthető, ellentétben az említett szabványokkal [122]. A megfelelést nemzeti piacfelügyeleti hatóságok és akkreditált tanúsító szervezetek ellenőrzik, az Európai Bizottság pedig a szabályok harmonizálásáért, míg az ENISA a technikai támogatásért felel [68], [123].

A rendelet ugyan előrelépést jelent a hálózatba kapcsolt termékek kiberrezilienciájának javításában, de számos korláttal bír. Nem foglalkozik a járműspecifikus kommunikációs

protokollokkal (pl. CAN, LIN, FlexRay) és architekturális sajátosságokkal, a beszállítói auditálásra pedig nem biztosít részletes keretrendszert [124]. Nem hangolja össze megfelelően a járműipari szabványokat – különösen az ISO 21434-et – és a GDPR-t, mivel a CRA elsősorban a termékoldali biztonságra, nem pedig a felhasználói adatvédelemre koncentrál [125].

Bár a rendelet kockázatalapú megfelelésértékelést ír elő, konkrét módszertant nem határoz meg, ami a gyakorlatban formális megfeleléshez vezethet. A „one-size-fits-all" megközelítés ezért nem feltétlenül alkalmas a biztonságkritikus rendszerek, például a személygépjárművek esetében [126], [127]. Több szerző [128], [129] kiemeli, hogy a CRA nem tartalmaz explicit alapjogi értékelési mechanizmusokat, ami bonyolítja a GDPR-ral való összehangolást. Kritika érte továbbá a rendelet hatását a nyílt forráskódú szoftverfejlesztésre is, mivel az új kötelezettségek gátolhatják az innovációt [130].

Egyes elemzők [131] jogbizonytalanságra és az arányosság elvének hiányos érvényesülésére figyelmeztetnek, míg más tanulmányok szerint a kis- és középvállalkozások számára a megfelelés aránytalan erőforrásterhet jelenthet [132]. Bár a CRA fontos mérföldkő az EU digitális termékbiztonsági szabályozásában, jelenlegi formájában nem nyújt teljes körű megoldást a járműipari rendszerek és a felhasználói adatok védelmére. A hatékony alkalmazáshoz iparágspecifikusabb, technikailag részletesebb és a meglévő szabványokkal integráltabb végrehajtási keretrendszerre van szükség.

3.6. Következtetések

A tartalmi és összehasonlító elemzés alapján világosan kirajzolódik, hogy azok a szabályozások a leginkább relevánsak a vizsgálat szempontjából, amelyek egyszerre helyezik fókuszba a személygépjárműveket mint hálózatba kapcsolt, digitális termékeket, és egyúttal érdemi védelmet nyújtanak a kiberbiztonsági fenyegetésekkel szemben. Kiemelkedik ezek közül az ISO/SAE 21434, amely iparágspecifikus megközelítést alkalmazva részletes technikai követelményrendszert nyújt a járművek kiberbiztonsági mérnökségéhez. Hasonlóan, az ISO 26262 a funkcionális biztonság területén képvisel mélyreható szabályozást, különösen a szenzorfúzió és hibakezelési protokollok szintjén. Az ISO/IEC 27001 ugyan nem kifejezetten az autóiparra vonatkozik, de a teljes szervezeti működésre kiterjedő információbiztonsági irányítási rendszer (ISMS) kialakításával,

illetve auditálható struktúrájával érdemben támogatja a megfelelőséget, különösen az ellátási lánc kockázatainak kontrolljában.

A Cyber Resilience Act (CRA) szintén a vizsgálati körbe tartozik, mivel jogilag kötelező és közvetlenül érvényesíthető szabályozás, amely a hálózatra kapcsolt digitális termékek – így a szoftveralapú járműfunkciók – biztonságát és fenntarthatóságát szabályozza. Bár nem iparágspecifikus, hatóköre a gépjárművek firmware- és távoli hozzáférési felületeire is kiterjed, és a beszállítói láncra vonatkozó transzparenciakövetelmények révén fontos kapcsolódási pontokat kínál. A CRA ugyan nem helyettesíti a GDPR-t, de kiegészíti azt a biztonsági hibákból fakadó adatvédelmi incidensek kezelésében.

Az R155 és R156 rendeletek a típusjóváhagyáshoz kötődő megfelelőségi követelményekkel elsősorban új járműmodellekre vonatkoznak, így kevésbé alkalmasak átfogó szervezeti vagy visszamenőleges elemzések alapjául, noha hatályosságuk és szabályozási mélységük vitathatatlan. Az elemzési szempontok mentén ezért a további vizsgálat fókuszát elsősorban az ISO 27001, az ISO/SAE 21434, az ISO 26262, valamint a jogilag kötelező és technikai értelemben is részletes előírásokat tartalmazó CRA szabályozásra helyezem, mivel ezek strukturált, alkalmazható és részben átfedő követelményrendszere közvetlenül kapcsolódik az értekezésben megfogalmazott célokhoz és problématérhez.

Fontos kiemelni, hogy az elemzett szabályozások és szabványok között jelenleg nincs olyan, amely átfogóan és kimerítően kezelné, hogy az internetkapcsolattal rendelkező járművek milyen típusú adatokat, milyen jogcímen, pontosan milyen céllal és feltételekkel oszthatnak meg különböző külső szereplőkkel – így például városüzemeltető szervezetekkel, márkaszervizekkel, biztosítókkal vagy flottakezelőkkel. E szereplők adatkezelési tevékenysége kapcsán is elsősorban általános adatvédelmi keretek (pl. GDPR) érvényesülnek, amelyek azonban nem térnek ki a járműadat-ökoszisztéma speciális viszonyrendszerére és az ezekből fakadó sajátos kockázatokra. Különösen problémás, hogy a gépjárművezetők rendszerint nem, vagy csak részlegesen kapnak átlátható, érthető tájékoztatást arról, hogy járművük milyen adatokat továbbít, kikhez és milyen célból – miközben hozzájárulásuk is sokszor pusztán formális, például általános szerződési feltételekbe rejtve történik meg. Mindezek miatt az adatmegosztás átláthatósága és a felhasználói jogok tényleges érvényesülése jelentősen korlátozott az okosjárművek ökoszisztémájában.

A funkcionális összehasonlító elemzés eredményei alapján megállapítható, hogy a jelenlegi európai szabályozási környezet csak részleges és foltszerű védelmet nyújt az internetkapcsolattal rendelkező személygépjárművek életciklusa során jelentkező fenyegetésekkel szemben. Az elemzés rávilágított arra is, hogy a szabályozások lefedettsége és gyakorlati kikényszeríthetősége jelentős hiányosságokat mutat, mivel azok vagy kizárólag a gyártókra, vagy csak bizonyos alrendszerekre koncentrálnak, így nem képesek átfogó, egységes védelmet biztosítani a teljes jármű-ökoszisztéma számára. Mindezek a kutatási eredmények egyértelműen megalapozzák az 1. Tézis megfogalmazását, miszerint az Európai Unió jelenlegi szabályozási rendszere nem nyújt kellően átfogó és hatékony információbiztonsági védelmet a személygépjárművek számára.

A kutatás további, második kérdése – a kockázatelemzési módszerek korlátainak vizsgálata – tekintetében az elemzés több, rendszerszintű problémát is felszínre hozott. Ezek részletes bemutatására és értékelésére azonban a későbbi fejezetekben, valamint a kvalitatív interjúk eredményei alapján kerül sor; a vonatkozó következtetések a disszertáció második tézisében kerülnek majd összegzésre.

4. EMPIRIKUS KUTATÁSI EREDMÉNYEK

Az empirikus kutatás célja az volt, hogy a korábbi tartalomelemzésen alapuló eredményeket a gyakorlatban is alátámassza, és mélyebb válaszokat adjon a kutatási kérdésekre, különös tekintettel a jelenleg alkalmazott járműipari kockázatelemzési módszerek gyakorlati korlátaira (K2). A vizsgálat során emellett kitértem arra is, hogy az internetkapcsolattal rendelkező járművek vásárlói mennyire tájékozottak a biztonsági kockázatokról és ezek a tényezők miként befolyásolják döntéseiket (K3), illetve hogyan jelennek meg a szabályozási elvárások a piaci szereplők szemszögéből (K1).

A fejezet a kvantitatív és kvalitatív módszertanokat egyaránt ötvöző kutatási megközelítést követ: egyrészt kérdőíves adatgyűjtés révén vizsgálja a felhasználói tudatosságot és informáltságot, másrészt szakértői mélyinterjúk segítségével elemzi a szabályozások és információbiztonsági gyakorlatok valós kihívásait. A kérdőíves kutatás elsődlegesen arra fókuszál, hogy az autótulajdonosok milyen ismeretekkel rendelkeznek járműveik adatküldési és -feldolgozási képességeiről, illetve hogy kaptak-e érdemi tájékoztatást ezen funkciókról. Ezzel szemben a szakértői interjúk elsősorban a kockázatelemzési folyamatok és a szabályozások gyakorlati alkalmazásának korlátait

vizsgálják, külön hangsúlyt helyezve arra, hogy a jelenlegi szabványok mennyiben felelnek meg az iparági kihívásoknak.

A kvalitatív módszertan szerepe ebben az esetben különösen jelentős, mivel az információbiztonsági gyakorlatok értékelése gyakran csak szakértői megítélés és tapasztalat alapján ragadható meg. A két vizsgálat együttes célja, hogy átfogó képet nyújtson a személygépjárművek adatvédelmi és kiberbiztonsági helyzetéről, és hozzájáruljon a szabályozási és technológiai hiányosságok azonosításához, különös tekintettel a kockázatelemzés aktuális problémáira.

4.1. Kérdőíves kutatás – a felhasználók percepciói az okos járművek kapcsán

A kérdőíves kutatás célja annak feltárása, hogy a személygépjármű-tulajdonosok mennyire rendelkeznek tudatos ismeretekkel járművük adatkezelési és adattovábbítási gyakorlatairól, különös tekintettel az internetkapcsolattal rendelkező járművek által végzett adatszolgáltatásra. A vizsgálat közvetlenül a K3 kérdéshez kapcsolódik, és azt vizsgálja, hogy a végfelhasználók milyen tájékoztatást kapnak a járműveik által gyűjtött és továbbított adatok természetéről, céljáról és lehetséges kockázatairól, képesek-e érdemben értékelni adatvédelmi kitettségüket.

A kérdőívben kiemelt szerepet kaptak azok a kérdések, amelyek a válaszadók technikai tájékozottságát mérik az adatküldési funkciókkal kapcsolatban: tisztában vannak-e azzal, hogy járművük képes-e hálózati kommunikációra, és hogy továbbít-e adatokat a gyártónak vagy más szereplőknek. Emellett a kutatás vizsgálja azt is, hogy a résztvevők kaptak-e bármilyen formális tájékoztatást az adatkezelésről (például adatvédelmi nyilatkozat, használati útmutató vagy szervizelési tanácsadás keretében), illetve hogy milyen mértékben tartják fontosnak az ilyen jellegű információk elérhetőségét. A vizsgálat középpontjában tehát nem csupán a technikai ismeretek állnak, hanem az ezekhez kapcsolódó felhasználói attitűdök és információs elvárások is, amelyek kulcsfontosságúak a személygépjárművek adatbiztonságával és az adatvédelmi megfeleléssel kapcsolatos társadalmi bizalom megértéséhez.

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 több fő kategóriára oszthatók. Az alapvető demográfiai információk rögzítése során a válaszadók életkorát és származási országát kérdeztem. A gépjárműtulajdonosi tapasztalatok és preferenciák témakörében olyan kérdések szerepeltek, mint hogy jelenleg rendelkezik-e a válaszadó személygépjárművel, milyen márkájú autót birtokolt legutóbb, illetve hogy hány autó van a család tulajdonában. Az okosautó-technológiával kapcsolatos tudatosság feltérképezésére azt vizsgáltam, hogy a kitöltők tisztában vannak-e azzal, hogy autójuk képes-e internetes kapcsolatra, vagy rendelkeznek-e okosautóval. Az adattovábbítás és adatvédelem tudatossága kérdéskörében a válaszadók arról nyilatkoztak, tudják-e, hogy járművük továbbít-e adatokat a gyártónak vagy harmadik félnek, illetve kaptak-e erről formális tájékoztatást. Az adatvédelem és kockázatérzékelés témájában nyitott kérdések segítettek feltárni, hogy a válaszadók milyen potenciális problémákat látnak abban, ha a jármű a tudtuk nélkül továbbít adatokat. Végül az autóválasztási preferenciák feltérképezésekor arra voltam kíváncsi, hogy a kitöltők milyen szempontok alapján választanak, illetve kerülnének bizonyos származási országú járműveket, és ennek milyen indokai lehetnek.

4.1.1. Mintavételi 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, az országok szerinti eloszlást a 14. táblázat mutatja be.

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).

A célcsoport kiválasztása során különböző kulturális hátterű célországokat bevonására törekedtem. Az elektromos személygépjárművek elterjedésében Norvégia vezető helye a világon megkérdőjelezhetetlen. Az elektromos személygépjárművek elterjedése terén Norvégia világelső: 2025 augusztusára közel egymillió elektromos autót regisztráltak az országban, és a piacvezető új modellek szinte kizárólag tisztán elektromos meghajtásúak [133]. 2024-ben az újonnan eladott személygépkocsik mintegy 89 %-a teljesen elektromos volt, ami egyedülálló arányt jelent a világon, és az okosjárművek elterjedésének is fontos indikátora [134]. 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 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

2. *táblázat - Top 7 nemzet megjelenése a mintában. Forrás: saját forrás.*

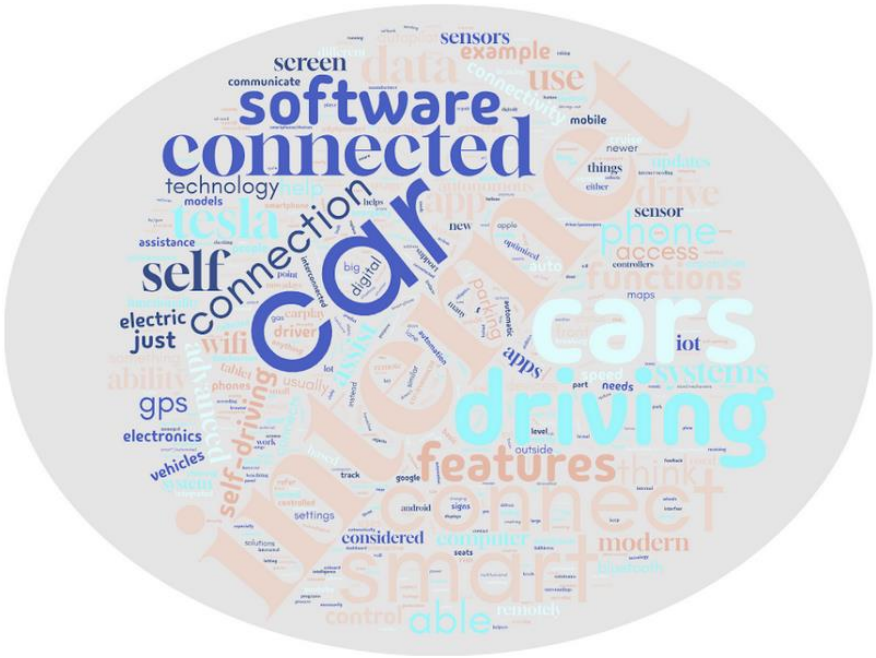
Összesen 29 országból érkezett válasz, köztük például Vietnámból, Mongóliából, Ukrajnából, Pakisztánból és a balti államokból is. A kisebb létszámú válaszadók Olaszországból, Lengyelországból, Észak-Macedóniából, Mexikóból és Thaiföldről kerültek ki, mindegyik országból egy-egy válasz érkezett.

4.1.2. 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 (esetleg hogy az autó vezeti önmagát az autópályán vagy rendelkezik a kapcsolt zenelejátszó alkalmazás preferenciaadataiaval, ami alapján következtetni tud a felhasználó hangulatára)? Ezeket a 7. Számú mellékletben található 13. táblázat szemlélteti.

A válaszadók szöveges válaszai alapján megkerestem azokat a kulcsszavakat amelyek jellegzetesen előfordulnak a válaszokban amellyel az okosautó fogalmát definiálják. A leggyakoribb kifejezéseket a 2. Ábrán látható szófelhővel mutatom be.

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.



2. ábra - Leggyakrabban előforduló kifejezések - Szófelhő. Forrás: saját forrás.

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 [135]. Egyik francia válaszadóm konkrétan úgy fogalmazott, hogy azért a francia járműveket preferálja, mivel ő maga is francia. Az eredményekből 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.

Ugyan a következő kérdés kifejezetten arra irányult hogy melyik országot preferálják, a válaszokból az derült ki, hogy többen fontosnak tartották már itt megemlíteni hogy mely

országból nem vásárolnának személygépjárművet, pl: „mindegy, csak ne kínai legyen” a jármű. A válaszokból készült diagram a 7. Számú melléklet 14.

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”).

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 válaszadók indoklásaiból az is kiderül, hogy milyen ok vagy okok miatt nem preferálják a megnevezett országokat. (7. Számú melléklet 15. ábra) 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 eredmény 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 7. Számú melléklet 16. és 17. táblázat).

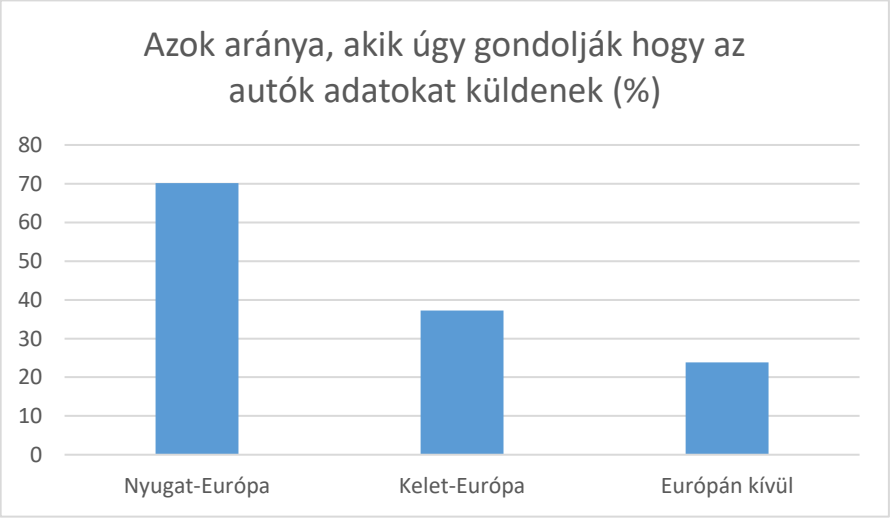
Az eddig elemzett válaszok alapján az általános hozzáállást, általános aggályokat próbáltam feltérképezni – anélkül, hogy az információbiztonság témakörét szóba hoztam volna, és ezzel befolyásoltam volna a megkérdezetteket. A kérdőív további részében azonban konkrétan is rákérdeztem, tartanak-e a válaszadók 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). A következő kérdésben rákérdeztem arra is hogy hány autó van a válaszadó családjában, valamint hogy mit gondol a családjában lévő személygépjárművek adatküldési szokásairól. A 7. Számú mellékletben az 18. és 19. ábrákon megtekinthető a válaszokat szemléltető diagram.

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.

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, melyeket a 3. ábra mutat be.



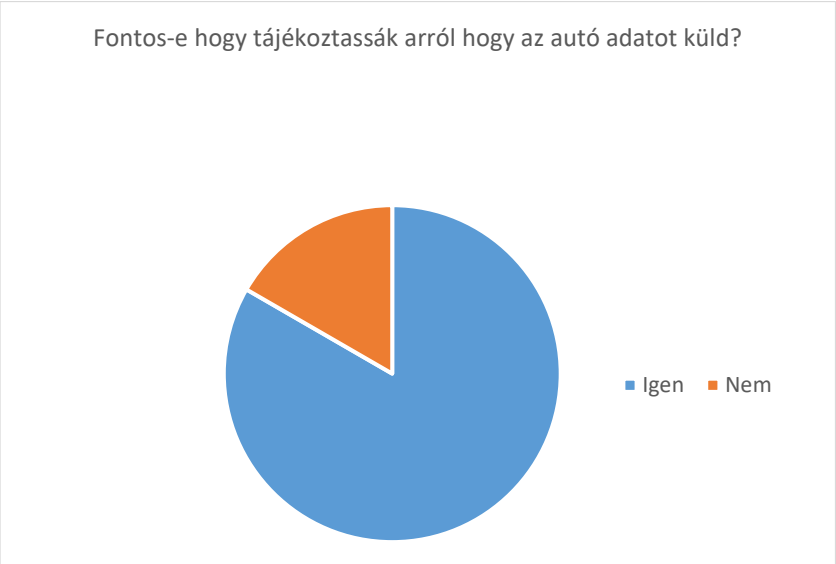
3. ábra - Azok aránya, akik úgy gondolják, hogy a személygépjárművek továbbítanak adatokat - származás szerinti bontásban. Forrás: saját forrás.

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, ezt a 4. ábra szemlélteti.

4. ábra - Válaszok arra a kérdésre vonatkozóan, hogy a személygépjárműtulajdonosok kaptak-e valaha tájékoztatást a jármű adattovábbítási folyamataira vonatkozóan. Forrás: saját forrás.

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. Az adatkiküldésről szóló tájékoztatás kapcsán régiós bontásban megállapítható, hogy kizárólag nyugat-európai válaszadók jelezték, hogy kaptak ilyen jellegű információt; kelet-európai és Európán kívüli válaszadók közül senki sem számolt be adatküldéssel kapcsolatos tájékoztatásról.

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. A válaszok eloszlását az 5. ábrán szemléltetem.

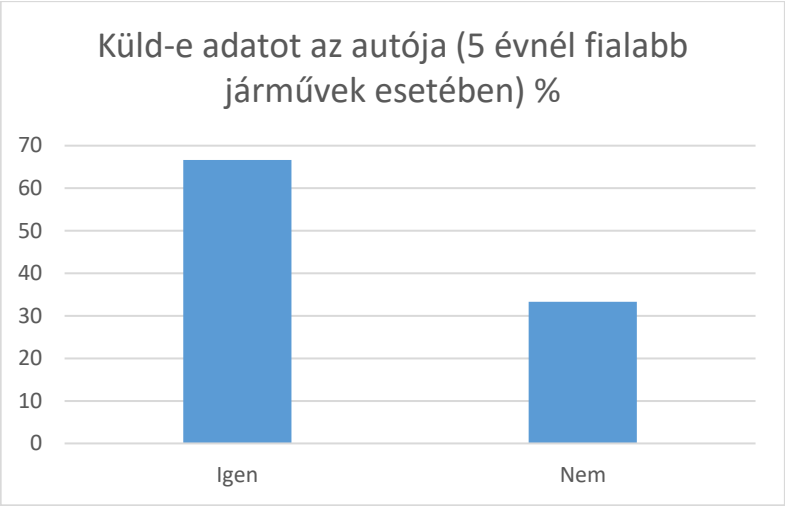


5. ábra - Az adattovábbítással kapcsolatos tájékoztatás fontossága a válaszadók szerint. Forrás: saját forrás.

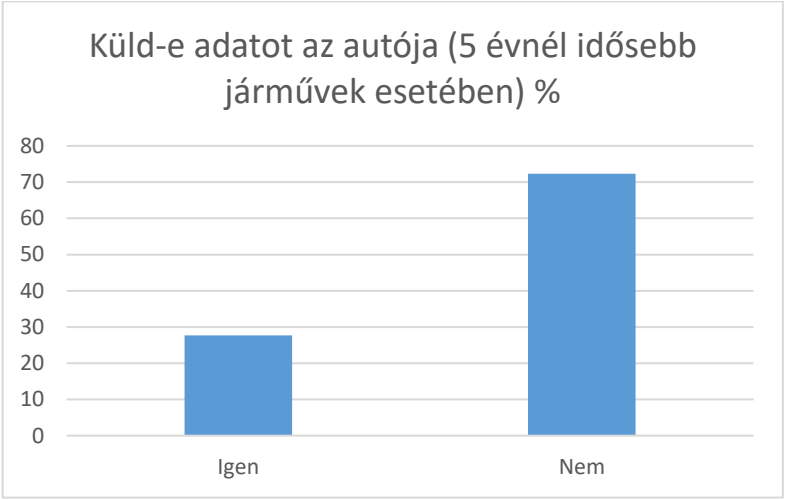
Az eredményekből látható, hogy a válaszadók nagy része fontosnak tartja, hogy ha az adattovábbítás megtörténik, akkor tájékoztatást kapjanak erről. Érdekes megfigyelni, hogy vannak olyan válaszadók is, akik ezt az információt nem tartják fontosnak, a kérdőív megalkotása során azonban ezt nem vettük figyelembe,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

Az adatkiküldéssel kapcsolatos tájékoztatás fontosságának megítélése földrajzi bontásban is vizsgálható. Az eredmények alapján minden régió Nyugat-Európa, Kelet-Európa és Európán kívüli országok válaszadói egyöntetűen fontosnak tartják, hogy tájékoztatást kapjanak az adatkiküldésről, 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 (6. és 7. ábra):



6. ábra - Az adattovábbítással kapcsolatos tájékoztatás fontossága a válaszadók szerint. Forrás: saját forrás.



7. ábra - Az adattovábbítással kapcsolatos tudatosság 5 évnél idősebb járművek esetén. Forrás: saját forrás.

Bár ebben az összefüggésben a pontos személygépjárműtípust nem tudtam vizsgálni, mert azt 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. A telematikai rendszerek elterjedtségét alátámasztja, hogy a 2023-ban eladott új gépjárművek mintegy 75 %-a már OEM-beágyazott telematikai rendszert tartalmazott. Ez azt jelenti, hogy az öt évnél fiatalabb járművek esetében szinte biztos, hogy az autó képes adatokat továbbítani valamilyen formában. A telematikai rendszerek nem csupán a gyártóhoz közvetítenek adatokat, hanem harmadik felek számára is hozzáférhetővé válhatnak. Több autógyártó – köztük a General Motors, Hyundai, Kia, Mitsubishi és Subaru – delegált adatokat küld vagy oszt meg LexisNexis vagy Verisk adatbrókerek

számára, amelyeket aztán biztosítók használnak fel a vezetői viselkedés elemzésére és a biztosítási díjak testreszabására [136], [137]. E speciális platformok révén "valós világban szerzett vezetési viselkedési adatokat" osztanak meg akár több tízmillió jármű esetén [138].

4.1.3. A kérdőív megbízhatóságának vizsgálata

A megbízhatóság vizsgálatához alkalmazott szokásos mutatók, mint a Cronbach-alfa [139] és a Guttman-féle lambda, [140] jelen esetben korlátozottan alkalmazhatók. Ezek az értékek akkor relevánsak, ha a kérdések egyetlen, közös konstruktumot mérnek. A jelen kérdőív célja azonban a *mixed methods* módszertant követve több, egymással csak nem erősen korreláló szempont vizsgálata volt. A Cronbach-alfa értéke a kérdőív esetén az elfogadható határérték körül mozgott, amely megerősíti a várakozásokat: a kérdések nem szoros konzisztenciát mutatnak, és ez metodikailag indokolt is volt.

A válaszok statisztikai érvényességének további biztosítása érdekében Mahalanobis-távolságokat [141] is számítottam, hogy azonosítsam a kiugró válaszokat. A 95%-os konfidenciaintervallumon kívül eső eseteket manuálisan újraértékeltem, és indokolt esetben kizártam az elemzésből.

Az így megtisztított adatbázisban 289 érvényes válasz maradt. Bár ez nem tekinthető reprezentatív mintának, a cél az általános tendenciák és attitűdök feltérképezése volt, amelyhez ez a mintanagyság megfelelő megbízhatóságot biztosít. A numerikus és kvalitatív ellenőrzések alapján az adatokat összességében megbízhatónak és elemzésre alkalmasnak tekintettem. A kérdőív megbízhatóságára vonatkozó számításokat a GitHub platformon tettem közzé[9]. A megbízhatóság értékelésének részletes menetét a 8. melléklet tartalmazza.

4.2. A kérdőíves eredmények nemzetközi szakirodalommal való összevetése

Mivel a kutatás mintanagysága korlátozott volt, kérdőíves kutatás során kapott válaszok értelmezéséhez elengedhetetlen a nemzetközi szakirodalmi háttér áttekintése. Ezáltal megállapítható, hogy az eredmények mennyiben tükröznek általános trendeket az okosautók adatvédelmi tudatosságával kapcsolatban, illetve milyen egyedi eltérések figyelhetők meg a mintában. A módszertani fejezetben bemutatott indoklásnak

[9] Saját forrás. URL: https://github.com/hhenrietta/smarcar_survey (frissítve: 2025.08.10)

megfelelően a primer eredményeket nemzetközi szakirodalmi adatokkal vetettem össze. Ez a lépés nemcsak az eredmények értelmezhetőségét, hanem a kutatás érvényességét is erősíti, és lehetőséget teremt a bemutatott tapasztalatok szélesebb, nemzetközi kontextusban való értékelésére.

4.2.1. Adatvédelmi és adatbiztonsági kihívások okosautókban

Ez a rész a kérdőíves kutatás azon kérdéseihez kapcsolódik, amelyek azt vizsgálták, hogy a felhasználók mennyire vannak tisztában az internetkapcsolattal rendelkező járművek által generált adatok típusával és mennyiségével, illetve a kapcsolódó adatvédelmi és adatbiztonsági kockázatokkal. Az okosautók működéséből eredő nagymértékű adatgyűjtés kiemelt jelentőséggel bír, hiszen ezek az adatok személyes és érzékeny információkat tartalmaznak, melyek védelme és megfelelő kezelése alapvető elvárás az érintett szereplők felé.

Az internetkapcsolattal rendelkező modern járművek működésük során egyes becslések szerint akár 25 gigabájt adatot továbbítanak óránként [142]. Ezek az adatok jelentős része személyes jellegű információ a jármű vezetőjéről vagy utasairól [143]. Az adatok között megtalálhatók a jármű műszaki állapotára, a vezetési mintázatokra, helymeghatározásra, biometrikus azonosítókra és kommunikációs metaadatokra vonatkozó információk is. A szakirodalmi konszenzus szerint az adatvédelem és adatbiztonság kérdésköre kiemelt problémát jelent az összekapcsolt járművek esetében [143]. Jelenleg hiányoznak az egységes szabványok és protokollok, amelyek biztosítanák az adatok end-to-end védelmét [143].

4.2.2. A felhasználók tudatossága és tájékozottsága az adatkezeléssel kapcsolatban

Ez az alfejezet a kérdőív azon kérdéseire reflektál, amelyek a felhasználók informáltságát, tájékozottságát és attitűdjeit mérték az autójuk adatkezelési gyakorlatairól. Fontos, hogy a végfelhasználók tudják, milyen adataikat, milyen célból és kik kezelik, illetve mennyire tartják biztonságosnak vagy átláthatónak az adatkezelési folyamatokat. Ennek feltárása segíthet abban, hogy azonosíthatók legyenek azok a területek, ahol a gyártók vagy a szabályozók további edukációra, pontosabb tájékoztatásra szorulnak, illetve rávilágít a fogyasztói bizalom szintjére és az ebből fakadó kockázatokra is.

A felhasználók adatvédelmi tudatossága az internetkapcsolatú járművek terén még több kutató szerint is fejletlen [144], [145]. A legtöbb járművezető nincs teljesen tisztában

azzal, milyen adatokat gyűjt és továbbít a járműve [144]. Empirikus kutatások kimutatták, hogy a gyártók által adott tájékoztatás gyakran nem megfelelő, ami a fogyasztók bizonytalanságához vezet [144]. Fókuszcsoportos interjúk szerint a felhasználók körében közöny és bizalmatlanság tapasztalható az adatkezeléssel kapcsolatban [144]. Szakértők szerint a felhasználók edukációja, valamint technikai eszközök (pl. alkalmazások) biztosítása elengedhetetlen a tudatos adatkezelés előmozdításához [145].

4.2.3. A kérdőíves kutatáshoz kapcsolódó nemzetközi szakirodalmi háttér

Több nemzetközi kutatás is rámutatott arra, hogy a fogyasztók adatvédelmi tudatossága az internetkapcsolatú járművek esetében még kialakulóban van. Smith és munkatársai. (2022) [146] szerint a legtöbb felhasználó nem teljesen érti, hogy milyen típusú adatok gyűjtésére kerül sor és milyen kockázatokkal jár ezek kezelése. Müller és munkatársai. (2023) [147] pedig kimutatta, hogy a fogyasztók hajlandósága adataik megosztására szignifikánsan csökken, ha a tájékoztatás hiányos vagy nem transzparens.

Shin és Park (2021) [148] empirikus kutatásukban kérdőíves felméréssel vizsgálták az okosautó-felhasználók adatvédelmi attitűdjeit. Eredményeik szerint a fogyasztók adatvédelmi aggodalmai közvetlen hatással vannak az adataik megosztására való hajlandóságukra. A bizalom és az észlelt kontrollérzet növeli az adatok megosztására való készséget, míg az adatvédelmi aggályok ezt jelentősen csökkentik. A kutatás 168 válaszadót vont be, és strukturált modellezéssel (SEM) elemezte az összefüggéseket.

A saját kérdőíves kutatás eredményei hasonló tendenciákat mutatnak. A válaszadók többsége nem volt tisztában azzal, hogy járműve milyen adatokat gyűjt, és aggodalmukat fejezték ki az adatkezelés átláthatóságának hiánya miatt. Ugyanakkor a saját minta eredményei szerint a bizalom szerepe kevésbé volt meghatározó tényező, mint Shin és Park (2021) [148] eredményeiben, és inkább az információhiány dominálta a válaszadók attitűdjeit.

4.2.4. 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, 25,7% pedig, 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 alapján megállapítható, hogy az „okosautó" fogalma rendkívül sokféleképpen jelenik meg a válaszadók gondolkodásában. Egyesek az internetkapcsolat megléte miatt sorolják autójukat ebbe a kategóriába, mások a fejlett szoftveres környezetet, illetve a mesterséges intelligencia technológiáját emelik ki, míg akadnak, akik elsősorban a kényelmi funkciókhoz kötik az „okosságot". Noha a folyamatos adatküldési és -fogadási képesség sem ismeretlen a kitöltők számára, ezt a tulajdonságot csak kevesen tartják igazán lényegesnek az okosautó definíciójában, vagyis önmaguktól ritkán gondolnak bele ennek jelentőségébe. A válaszokból egyértelműen kirajzolódik az is, hogy a személygépjárművek származási országa szerinti elutasítottság különösen markáns Kína esetében, főként a nyugat-európai válaszadók körében. Ezen attitűd elsődleges oka geopolitikai természetű, a minőségi fenntartások bár jelen vannak, inkább másodlagos szerepet játszanak az elutasításban. Amikor a kérdőív konkrétan rákérdezett arra, hogy a jármű adatokat továbbíthat, a válaszadók többsége felismerte és elfogadta a kockázatok létezését. Ugyanakkor, ha a saját autójuk adattovábbítási képességéről volt szó, kevésbé tekintették ezt negatívumnak, mint amikor általánosságban, például a család tulajdonában lévő gépjárművekre kellett gondolniuk. Szintén jellemző, hogy sokan nincsenek teljesen tisztában azzal, hogy járművük egyáltalán adatokat továbbít, és még kevesebben tudják, hogy ezek az adatok akár harmadik félhez is eljuthatnak. Mindezek ellenére a legtöbb válaszadó aggodalmát fejezte ki az adatgyűjtéssel járó kockázatokkal kapcsolatban.

A kérdőíves kutatás elemzése során a K3 kutatási kérdésre adott válaszok egyértelműen kirajzolták azt a mintázatot, hogy az internetkapcsolattal rendelkező járművek vásárlói jellemzően nincsenek kellő mértékben tájékoztatva a járművek által végzett adattovábbítás tartalmáról, gyakoriságáról és kockázatairól. A válaszadók többsége az okosautók kényelmi és innovatív funkcióit emelte ki, miközben a biztonsági kockázatok, illetve az adatkezelési folyamatok átláthatósága háttérbe szorult. Ez a megállapítás közvetlenül a K3 kutatási kérdésből levezetett

T3 tézishez vezetett, amely kimondja, hogy az okosjárművek vásárlói nem kapnak megfelelő tájékoztatást a biztonsági kockázatokról, és a technológiai fejlődésből eredő kényelmi funkciók dominanciája miatt nem fordítanak kellő figyelmet ezekre a veszélyekre. A nemzetközi kutatásokkal való összevetés tovább erősíti ezt a következtetést: globálisan is hiányosságok mutatkoznak az adatvédelmi tájékoztatás és a felhasználói tudatosság terén, valamint általános jelenség, hogy a felhasználók információhiánnyal és bizalmatlansággal néznek szembe az adatkezelés kapcsán. A saját kutatás eredményei így nemcsak a bemutatott országokra nézve, hanem nemzetközi viszonylatban is alátámasztják a T3 tézis megalapozottságát.

4.3. Mélyinterjúk – Hazai szakértők tapasztalata

A jelen fejezet célja, hogy kvalitatív módszertannal készült szakértői mélyinterjúk segítségével árnyaltabb képet adjon a személygépjárművek információbiztonságának gyakorlati kihívásairól, különös tekintettel azokra a kérdésekre, amelyek pusztán dokumentumvizsgálattal nem válaszolhatók meg. A vizsgálat fókuszában a második kutatási kérdés (K2) áll, vagyis annak feltárása, hogy a jelenleg alkalmazott autóipari kockázatelemzési módszerek milyen korlátokkal küzdenek az internetkapcsolattal rendelkező járművek információbiztonsági kockázatainak kezelésében. Emellett a szakértői tapasztalatok hozzájárulnak az első (K1) és harmadik (K3) kutatási kérdés további megértéséhez is, például a szabályozási környezet hatékonyságának és a felhasználói tájékoztatásnak a gyakorlati aspektusait illetően.

A mélyinterjúk célja, hogy feltárják: miként jelennek meg a szabályozási keretek, a kockázatelemzés módszertani kihívásai, illetve az információbiztonsági gyakorlatok a hazai szakértők mindennapi tapasztalataiban. Kiemelt jelentőségű kérdés, hogy az iparági szereplők mennyire tartják egységesnek és átláthatónak a jelenlegi értékelési rendszereket, valamint milyen szubjektív vagy tapasztalati elemek játszanak szerepet a biztonsági szintek meghatározásában. A kutatás tehát a szakértői nézőpontok segítségével keresi a választ arra, hogy a szabványok és jogszabályok mennyiben tudják támogatni vagy éppen akadályozni az internetkapcsolatra képes járművek kockázatainak valódi, átfogó kezelését..

4.3.1. Mintavétel

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 [22]. Ennek következtében kizártam a nagy mintán elvégzett statisztikai módszerek alkalmazását.

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 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 [149]. 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 [150].

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.

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, 30 főből álló csoport szűkítésére. A kutatásban résztvevő 15 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.

Az interjúalanyok válaszaiból kiderül, hogy nyolc válaszadó dolgozott már valamilyen járműiparral kapcsolatos információbiztonsági projekten, feladatkörben, míg hét személy nem rendelkezik ilyen tapasztalattal. Ennek okán csak az előbbi nyolc személy számára tettünk fel iparágspecifikus, kifejezetten járműipari szabványokra vonatkozó kérdéseket.

4.3.2. Standardizált feltételek

A szakértői interjúk tanúsága szerint az információbiztonsági megfelelés értékelésekor a legnagyobb kihívást az jelenti, hogy hiányoznak a fenyegetettségi szintek objektív, standardizált összehasonlítására alkalmas módszerek. Nemcsak az iparági metrikák egységesítésének hiánya okoz problémát, hanem az is, hogy a cégek számára kevés elérhető, átfogó módszertan, egyértelmű hatósági útmutató vagy egységes értelmezési segédlet áll rendelkezésre. A szervezetek így gyakran kényszerülnek arra, hogy minden auditciklusban saját maguk alakítsák ki a fejlődés mérésére és a biztonsági szintek meghatározására vonatkozó szempontokat, amelyeknek nem mindig van valós iparági vagy hatósági alapjuk.

Tovább nehezíti a helyzetet, hogy az auditálások lefolytatásában is nagy eltérések tapasztalhatók. Az auditorok kapacitásai és felkészültsége sokszor eltérő, az auditmódszertanokat pedig nem szabályozzák szigorú, egységes előírások, így az auditok minősége erősen változó lehet. Bizonyos esetekben előfordul, hogy egy felületes, kevéssé részletes módszertan mellett is megfelel a szervezet, miközben valós védelmi hiányosságok maradnak rejtve.

A szakértők szerint mindezt tovább súlyosbítja, hogy a különböző szabványok és szabályozások gyakran átfedésben vannak egymással, vagy éppen lényeges területeken nem adnak kielégítő válaszokat a szervezetek problémáira. Ez jelentős adminisztratív terhet ró a vállalatokra, amelyek emiatt egyre szkeptikusabban viszonyulnak az újabb szabályozásokhoz. Sok esetben, ha tehetik, halogatják a kötelező előírások bevezetését is, vagy elkerülő magatartást folytatnak, amennyiben erre lehetőségük nyílik.

A szakértői interjúk során felmerült, hogy a modern személygépjárművek – az összetett szenzorrendszereknek és hálózati kapcsolódásnak köszönhetően – gyakorlatilag az IoT-eszközök közé sorolhatók információbiztonsági szempontból. A megkérdezettek többsége ezért úgy véli, hogy a gépjárművekre is célszerű lenne kiterjeszteni az IoT-berendezésekre vonatkozó biztonsági szabványokat, szabályozásokat és auditgyakorlatokat. Ugyanakkor hangsúlyozták, hogy a járművek rendszerszintű komplexitása miatt az ilyen megközelítés nem lehet pusztán komponensalapú: fennáll a veszélye annak, hogy egyes alkatrészek kimaradnak a védelmi fókuszból. Az egyik interjúalany a korábban bemutatott ISO/SAE 21434 szabvánnyal kapcsolatban kiemelte, hogy bár az jelentős előrelépést jelent az elektronikai biztonság terén, mivel az egyes elemekre fókuszál a teljes rendszer helyett, ezért nem nyújt átfogó megoldást. Amennyiben tehát az IoT-eszközökre érvényes szabványokat kívánjuk alkalmazni a személygépjármű egyes részeire, ezt a lefedettséggel összefüggő kockázatot figyelembe kell venni. Ez is rávilágít arra, hogy az információbiztonságot rendszerszinten, integrált módon érdemes kezelni, nemcsak a szabályozások, hanem a gyakorlati ellenőrzések során is.

4.3.3. Kockázatelemzés, metrikák, adatbiztonság

A mélyinterjúk alapján az internetkapcsolattal rendelkező járművek adatbiztonsági kockázatainak értékelése jelenleg súlyos módszertani hiányosságokkal küzd. A szakértők szerint sem szervezeti, sem termékszinten nem létezik egységes, integrált kockázatelemzési módszertan, amely lefedné a modern okosjárművek komplex fenyegetéseit.

A jelenlegi gyakorlatban a kockázatelemzési modellek elkülönülten működnek: a szervezeti szintű (pl. CRAMM, ISO 27005) és a termékfókuszú (pl. TARA) megközelítések között nincs valódi integráció. A próbálkozások gyakran bonyolult, nehezen karbantartható táblázatos rendszerekben merülnek ki, amelyek a gyakorlatban nem bizonyulnak hatékonynak.

A szakértők kiemelték, hogy hiányzik egy olyan integrált módszer, amely egyesíti a szervezeti és termékszintű kockázatelemzést, és figyelembe veszi a járműipar sajátos működési környezetét. Egy ilyen keretrendszer nemcsak a belső folyamatok összehangolását segítené, hanem az ökoszisztéma-szintű veszélyek azonosítását is lehetővé tenné.

Az IoT-alapú technológiák terjedésével különösen fontos lenne az olyan iparágspecifikus kockázatelemzés, amely figyelembe veszi a kis erőforrás-igényű kommunikációs protokollok és titkosítási megoldások sajátosságait. Jelenleg a döntések többnyire tapasztalati alapon, nem pedig összehasonlítható metrikák szerint születnek.

A szabályozási környezet töredezettsége tovább nehezíti az egységes szemlélet kialakítását. Az átfedő előírások és hiányos hatósági útmutatások miatt a megfelelés gyakran formálissá válik, az auditok minősége pedig változó. A beszállítói láncban ráadásul korlátozott az információáramlás, mivel a beszállítók csak ritkán kötelesek részletes biztonsági adatokat megosztani a gyártókkal.

A szakértői visszajelzések megerősítik a K2 kutatási kérdésben megfogalmazott problémát: a jelenlegi kockázatkezelési módszerek nem alkalmasak a hálózatba kapcsolt járművek szervezeti és technikai kockázatainak integrált kezelésére, és hiányzik az egységes, átlátható értékelési keret, amely alapul szolgálhatna a jövőbeli szabályozási és auditálási gyakorlatokhoz.

4.3.4. Megoldási javaslatok

A szakértői interjúk számos hiányosságra hívták fel a figyelmet. A leggyakrabban említett problémák közé tartozott a járművek növekvő komplexitása, a szoftvertámogatás korlátozottsága, a szervizfolyamatok átláthatatlansága, valamint az, hogy a jelenlegi szabályozások nem nyújtanak átfogó védelmet a járművek teljes életciklusára. A kockázatok az értékesítést követően is fennmaradnak – a használat, szerviz, tulajdonosváltás és selejtezés során egyaránt.

A szakértők hangsúlyozták, hogy az életciklus-szemlélet megvalósításához nemcsak a gyártók, hanem az utópiaci szereplők – márkakereskedések, szervizek, flottakezelők, bontók – bevonása is szükséges. Ők találkoznak először a felhasználókkal és adataikkal, ezért kulcsszerepük van a szabályozások gyakorlati érvényesítésében és a felhasználók edukálásában. Többen javasolták egy folyamatosan frissülő, fejlesztési életciklust is lefedő kockázatelemzési rendszer létrehozását, amely nemcsak a gyártókra, hanem a teljes járműipari ökoszisztémára kiterjed. Bár az ISO 26262 és az ISO/SAE 21434 fontos előrelépések, egyik sem biztosít teljes körű, összehasonlítható megközelítést; a gyártók által alkalmazott saját módszertanok fragmentálttá teszik a kockázatkezelést.

A felhasználói oldal tekintetében a szakértők szerint az autóvásárlók többsége nem kap megfelelő, közérthető tájékoztatást az adatkezelési gyakorlatokról és kockázatokról. A

kényelmi funkciók iránti érdeklődés és az információhiány miatt a biztonsági szempontok háttérbe szorulnak, a felhasználók nincsenek tisztában adataik kiszolgáltatásának következményeivel. A megoldást a szakértők többsége egy egységes, központi hatóság létrehozásában látná, amely koordinálná a járműipari szabványok alkalmazását és fejlesztését, iránymutatásokat és jógyakorlatokat adna ki, valamint módszertani és oktatási támogatást nyújtana az iparági szereplőknek. A szervezetnek hatósági jogosítványokkal és szankcionálási lehetőséggel is rendelkeznie kellene a szabályozások tényleges érvényesítéséhez.

Az interjúk alapján a jövőbeli fejlesztési irányokat egy többrétegű megközelítés határozza meg, amely magában foglalja a kockázatkezelési módszertanok egységesítését, a szabályozás központi koordinációját, az utópiaci szereplők folyamatos oktatását és aktív bevonását, valamint a felhasználók edukációját és az átláthatóság növelését. A szakértői tapasztalatok megerősítik a K2 és K3 kutatási kérdések során feltárt problémákat: a jelenlegi kockázatelemzési módszerek széttagoltak, az erőforráshiány és a standardizálás hiánya miatt a gyakorlatban gyakran formálissá válnak, a valódi fenyegetéseket pedig nehezen fedik fel. Emellett a felhasználói tájékozatlanság és a szabályozói koordináció hiánya rendszerszintű kockázatot jelent az okosjárművek adatbiztonságára.

4.4. Következtetések

Az empirikus kutatás eredményei mindhárom vizsgált területen releváns bizonyítékokat szolgáltattak: a szabályozási környezet továbbra sem képes átfogó és egységes védelmet garantálni; a kockázatelemzési módszerek széttagoltak, nehezen integrálhatók és kevéssé ellenőrizhetők; a felhasználók információhiánya és az ebből fakadó tudatosság hiánya pedig súlyosbítja a helyzetet. A szakértői interjúk és a kérdőíves kutatás tapasztalatai alapján a kutatási kérdésekre adott válaszokból fokozatosan, az empirikus bizonyítékok mentén formálódtak meg a dolgozat új tézisei. A kockázatelemzési gyakorlatok elemzése során egyértelműen kirajzolódott, hogy a jelenleg alkalmazott módszerek nem képesek objektív, egységes és átlátható értékelési rendszert nyújtani az internetkapcsolattal rendelkező járművek komplex információbiztonsági kockázatainak kezelésére. A szervezeti és termékszintű megközelítések elkülönülten léteznek, integrált módszertan hiányában pedig a szabályozás és az ellenőrzés is széttagolt marad.

A mélyinterjúk során feltárt szakértői tapasztalatok és a gyakorlati alkalmazás hiányosságai tették lehetővé, hogy a kutatási kérdésből konkrét tézis szülessen: a

szabályozások által elvárt kockázatelemzési módszerek jelenleg nem alkalmasak az internetkapcsolatra képes személygépjárművekkel kapcsolatos összes kockázat kezelésére, mivel vagy csak a járműre, vagy csak a szervezetre fókuszálnak, és használatukat nem ellenőrzi egységes hatóság (T2).

Hasonló módon, a felhasználók adatvédelmi tudatosságának vizsgálata során szerzett tapasztalatok, valamint a kérdőíves kutatás eredményei alapozták meg a T3 tézis megfogalmazását. A válaszadók többsége nincs megfelelően informálva az okosjárművek adatgyűjtési és adattovábbítási gyakorlatáról, az adatbiztonsági kockázatokat kevéssé érzékelik, és döntéseiket inkább a kényelmi, mintsem a biztonsági szempontok befolyásolják. Ezek az eredmények, a szakirodalmi összevetéssel együtt, lehetővé tették annak megállapítását, hogy az internetkapcsolatra képes járművek vásárlói nem kapnak megfelelő tájékoztatást a biztonsági kockázatokról, elsősorban a technológiai fejlődésből adódó kényelmi funkciókra koncentrálnak, így nem fordítanak figyelmet a kockázatokra (T3).

5. AZ ADATKÜLDÉS PROTOKOLLJAINAK VIZSGÁLATA

Az értekezés ezen fejezete azt vizsgálja, hogy az internetkapcsolattal rendelkező járművekben alkalmazott kommunikációs protokollok mennyire képesek biztosítani a személyes és bizalmas adatok védelmét, illetve milyen kockázatokat hordoznak, amelyek a hagyományos technikai biztonsági intézkedésekkel sem mindig kezelhetők [151], [152]. Elsődleges célja, hogy választ adjon az értekezésben megfogalmazott negyedik kutatási kérdésre (K4), mely különös jelentőséggel bír, hiszen a személygépjárművek egyre összetettebb hálózati architektúrái és a járművek közötti, illetve külső rendszerekkel folytatott adatkommunikációk száma és komplexitása folyamatosan növekszik. A vizsgálat során arra törekszem, hogy feltárjam: a különböző kommunikációs protokollok miként teremthetik meg a lehetőségét rejtett, a hagyományos védelemi eszközökkel nehezen észlelhető adatcsatornák kialakulásának, illetve hogy mennyiben képesek a jelenlegi biztonsági megoldások az ilyen típusú fenyegetések kivédésére. A fejezet áttekintése révén árnyaltabb képet kaphatunk arról, hogy a protokollok tervezése és alkalmazása miként hat a járművek valós adatbiztonsági szintjére, valamint hogy milyen további technikai és szabályozási lépések lehetnek indokoltak a jövőben. A protokollok technikai sajátosságainak elemzése rávilágít arra, hogy e rendszerek akár rejtett, ellenőrizhetetlen adatcsatornák kialakulását is lehetővé

tehetik, vagy éppen milyen mértékben tudnak védelmet nyújtani ezek ellen [153]. Az alábbiakban részletesen bemutatom, miként kapcsolódnak a kommunikációs protokollok az adatbiztonság gyakorlati megvalósulásához a személygépjárművek világában.

Az elmúlt évtizedben az autóipar digitalizációja és a hálózatba kapcsolt járművek megjelenése alapjaiban változtatta meg a közlekedés, a gépjárműhasználat és az adatbiztonság viszonyát [154], [155]. Ma már nem csupán szoftverrel támogatott vezetési élményről beszélhetünk: a modern személygépjármű dinamikus, mozgó adatközponttá vált, amely folyamatosan szenzoradatokat, helymeghatározási információkat, képi és hangfelvételeket generál, dolgoz fel és továbbít a felhasználó, a gyártó és különböző szolgáltatók felé [156], [157]. Ez a fejlődés nemcsak új lehetőségeket nyitott meg a fejlett vezetéstámogató rendszerek (ADAS), a távdiagnosztika vagy az intelligens biztosítási termékek számára, de eddig soha nem tapasztalt információbiztonsági és adatvédelmi kockázatokat is teremtett [158], [159].

A járművek által generált adatok jelentős része rendkívül érzékeny, tartalmazhat információkat a vezető viselkedéséről, szokásairól, útvonalairól, a jármű aktuális tartózkodási helyéről, sőt, akár a jármű utasterében történő eseményekről is [160]. Az autók így egyszerre váltak a felhasználói élmény és a digitális kitettség eszközeivé – mindennapjaink digitális „szem- és fültanúivá” [161].

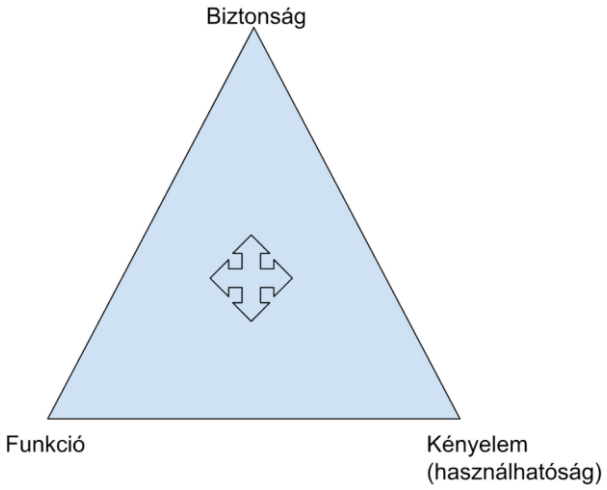
Az internetkapcsolatra képes gépjárművek adatkommunikációs architektúrája összetett, sokszereplős ökoszisztémában működik. Az adatok útja sokszor nem átlátható: elhagyva a járművet, különböző, akár földrajzilag távoli backend rendszerekhez, gyártói, biztosítói vagy külső szolgáltatók szervereihez jutnak el [154], [162]. Mindez jelentős átláthatósági és kontrollproblémákat vet fel mind a felhasználók, mind a szabályozók, mind az információbiztonsági szakemberek számára.

A digitalizált autóipar adatbiztonsági kihívásai az elmúlt években nem csupán elméleti szinten, hanem nagyon is valós, a sajtóban is megjelenő incidensek formájában kerültek a figyelem középpontjába. Egyik legismertebb példa a Tesla-ügy, amikor a Reuters tényfeltáró riportja alapján kiderült, hogy a fedélzeti kamerák által rögzített képekhez egyes dolgozók titkosítatlanul férhettek hozzá, sőt, privát célra is megosztották egymással [163]. Ez az eset rávilágított arra, hogy még a technológiai élvonalat képviselő gyártók számára is komoly kihívást jelent a szenzitív járműadatok feletti kontroll és a megfelelő információbiztonsági mechanizmusok implementálása [164].

De nem csupán a gyártók oldalán jelennek meg a kockázatok: a járműhasználók, tulajdonosok, sőt, a szabályozók is gyakran átláthatatlan adatkezelési és adattovábbítási folyamatokkal szembesülnek [158], [165]. A gépjármű tulajdonosának például ritkán van tényleges kontrollja afelett, hogy pontosan milyen adatok, mikor, hova és hogyan kerülnek továbbításra. A biztosítási ágazatban is elterjedt a vezetési szokásokhoz igazított díjszámítás (usage-based insurance), amelyhez elengedhetetlen a folyamatos telematikai adatgyűjtés – ám ezek az adatok szintén komoly adatvédelmi és visszaélési kockázatokat hordoznak [166], [167].

A fenti példák jól mutatják, hogy az internetkapcsolatra képes járművek adatkommunikációja nem pusztán technológiai kérdés, hanem üzleti, etikai és jogi dilemmákat is felvet [168].

A modern okosjárművek fejlesztése során a mérnököknek folyamatosan egyensúlyt kell találniuk a biztonság, a funkcionalitás, a felhasználói kényelem és a rendelkezésre álló technikai teljesítmény között. Ezt a dilemmát szemléletesen mutatja be a szakirodalomban is elterjedt „biztonság–funkció–kényelem” háromszög (8. ábra), amelyhez az IoT-eszközök esetén egyre gyakrabban társul negyedik tényezőként a teljesítmény (performance) is [169], [170]. Az ábra szerint a három, illetve négy sarokpont között mindig kompromisszumot kell kötni. Ha kizárólag a biztonságot helyezzük előtérbe, a rendszer használhatósága és funkcionalitása csorbulhat; ha viszont a kényelmi funkciókat vagy a maximális teljesítményt erőltetjük, az a biztonság rovására mehet [169]. Az autóiparban különösen érzékeny ez az egyensúly: a felhasználók elvárják a gyors reakciót, a valós idejű távoli funkciókat (pl. ajtónyitás, klíma vezérlés), miközben a biztonság és az adatvédelem nem lehet másodlagos szempont [155], [171].



8. ábra - Biztonság-funkció-kényelem háromszög. Forrás: saját forrás.

Az új autóipari trendek – például az OTA (over-the-air) szoftverfrissítések, a folyamatos telematikai adatgyűjtés, a felhasználóval való kétirányú kommunikáció – mind növelik a támadási felületek számát és a rendszerek komplexitását [172], [173]. Mindez szükségessé teszi, hogy ne csupán a végponti védelmi megoldásokra, hanem a járművekben alkalmazott kommunikációs protokollok elemzésére is különös figyelmet fordítsunk [174], [171].

A járművek kommunikációja ma már túlnyomórészt IP-alapú protokollokon keresztül zajlik [174]. A fedélzeti szenzoroktól érkező adatok különféle vezérlőegységeken (ECU), hálózati rétegeken keresztül jutnak el a külvilághoz, gyakran olyan protokollok segítségével, amelyeket eredetileg nem gépjárműipari, hanem általános IoT vagy internetes környezetre terveztek [175], [176].

A személygépjárművekben leggyakrabban használt alkalmazási rétegű protokollok közé tartozik a HTTP/HTTPS, az MQTT (Message Queuing Telemetry Transport) és a CoAP (Constrained Application Protocol), de előfordulnak klasszikus hálózati védelmi technológiák (pl. TLS, IPsec) vagy autóipari sajátosságok (pl. CAN, AUTOSAR SecOC) is [177], [178], [179]. Ezek a protokollok meghatározzák, hogy az adatforgalom miként strukturálódik, milyen védelmi mechanizmusok (titkosítás, hitelesítés, naplózás) valósulhatnak meg, illetve, hogy milyen támadási lehetőségek (például rejtett adatcsatornák) nyílhatnak meg a rosszindulatú szereplők előtt [180], [181].

A gyakorlatban tapasztalható, hogy a gyors fejlesztési ciklusok, a különböző gyártói és beszállítói megoldások, illetve a költségoptimalizáció miatt a protokollok implementációja és konfigurációja gyakran nem felel meg a legszigorúbb

információbiztonsági elvárásoknak [164], [173], [182]. Számos ismert sérülékenység és konfigurációs hiba származtatható közvetlenül a használt protokolloktól vagy azok nem megfelelő használatától – gondoljunk csak a titkosítás hiányára, brute-force védelem nélküli azonosításra, vagy a publikus témanevek kihasználására az MQTT-ben [178], [181].

5.1. Kommunikációs protokollok elemzése az OSI-modell mentén

Az internetkapcsolatra képes járművek, különösen a modern személygépjárművek adatkommunikációja rendkívül komplex, többrétegű hálózati architektúrára épül, amelyben különböző protokollok együttműködésével valósul meg az adatok továbbítása, feldolgozása és védelme [154], [175]. Az OSI (Open Systems Interconnection) modell adja a legalkalmasabb keretet a kommunikációs rétegek áttekintéséhez és a támadási felületek szisztematikus feltárásához [183], [184].

Az OSI-modell alkalmazása a járműkommunikáció biztonsági elemzésében lehetővé teszi, hogy minden egyes réteghez hozzá tudjuk rendelni az ott alkalmazott tipikus protokollokat, illetve a kapcsolódó támadási és védelmi lehetőségeket [165]. A személygépjárművek hálózataiban a protokollpaletta a fizikai rétegtől kezdve az alkalmazási rétegig terjed: a kommunikáció alapját általában a nagy sávszélességű vagy időzítési garanciákat adó fizikai és adatkapcsolati rétegbeli technológiák jelentik, mint például a dedikált autóipari Ethernet szabványok (mint a 100BASE-T1 és 1000BASE-T1), vagy a már hagyományosnak számító, megbízható vezérlőhálózatok, például a CAN (Controller Area Network) és a FlexRay [185], [186].

A hálózati rétegben a járművek egyre gyakrabban alkalmazzák az IPv4 vagy IPv6 protokollokat, illetve a 6LoWPAN-t is a szenzorhálózatok esetében, ahol a kis sávszélességű és erőforrás-korlátozott eszközök számára optimalizált IP-kapcsolatot kell biztosítani [187]. A szállítási rétegben legelterjedtebben a TCP és az UDP protokollok jelennek meg, ezekhez egyre gyakrabban társul valamilyen transzport szintű biztonsági mechanizmus, például a DTLS (Datagram Transport Layer Security) vagy az SCTP (Stream Control Transmission Protocol), amely elsősorban a megbízhatóságot és az adatfolyam-kezelést javítja, illetve a szenzitív adatok védelmét segíti elő [188]. A viszony réteg fontos szereplői közé tartoznak a különböző titkosítási és hitelesítési megoldások, mint például a TLS vagy a DTLS, amelyek megteremtik a biztonságos kapcsolat alapjait [189]. A megjelenítési rétegben egyre inkább terjednek az adatcserét támogató

formátumok és konverziók, így a JSON, a CBOR vagy a Protobuf, amelyek lehetővé teszik az eltérő rendszerek közötti adatértelmezést [190].

Az alkalmazási réteg adja azt a szintet, ahol már konkrét szolgáltatásokat, adatcserét, vezérlést, illetve felhasználói vagy gépi interakciót valósítanak meg (3. táblázat). Ebben a környezetben kiemelt jelentőséggel bírnak a webes és IoT-protokollok, így a HTTP, a HTTPS, az MQTT, a CoAP, illetve a WebSocket vagy különböző REST-alapú API-k [191], [192], [193].

OSI-réteg	Protokoll(ok)	Autóipari alkalmazási példa	Biztonsági relevancia / kockázat
1. Fizikai	100BASE-T1, CAN, FlexRay	ECU-k közötti alap kommunikáció	Fizikai támadások, kábelezési hibák
2. Adatkapcsolati	Ethernet MAC, CAN, MACsec	Üzenet keretezés, hibaellenőrzés	MACsec hiánya, CAN-busz sérülékeny
3. Hálózati	IPv4, IPv6, 6LoWPAN	Jármű-hálózat, backend elérés	IP-cím manipuláció, DoS támadások
4. Szállítási	TCP, UDP, DTLS	MQTT, CoAP, HTTP forgalom	Titkosítás hiánya, replay támadás
5. Viszony (Session)	TLS, DTLS, MQTT session	Biztonságos csatorna, session management	Lejárt tanúsítvány, session hijack
6. Megjelenítési	JSON, CBOR, Protobuf	Adattranszformáció, API kommunikáció	Sérülékeny parser, input validation
7. Alkalmazási	HTTP/HTTPS, MQTT, CoAP	OTA frissítés, telematikai kommunikáció	Rejtett csatornák, hitelesítés hiánya

3. táblázat - OSI rétegek szerinti kockázatelemzés. Forrás: saját forrás.

A legtöbb biztonsági és adatvédelmi incidens tapasztalati úton is az alkalmazási és szállítási réteghez köthető, ugyanakkor az alsóbb rétegek sajátosságai is közvetlenül befolyásolják a teljes kommunikációs lánc sérülékenységét [164], [179], [194]. A különféle protokollok egymásra épüléséből adódóan az egyes rétegek sérülékenységei gyakran láncreakciószerűen jelennek meg: például a TLS hiánya vagy helytelen konfigurációja a szállítási vagy megjelenítési rétegben lehetővé teszi a titkosítatlan HTTP, MQTT vagy CoAP forgalom lehallgatását, módosítását vagy rejtett csatornák létrehozását az alkalmazási rétegben [181], [195].

5.2. A részletesen vizsgált protokollok kiválasztásának indoklása

A modern, internetkapcsolatra képes járművek kommunikációs architektúrája napjainkra rendkívüli mértékben közelít az általános informatikai rendszerekhez: az autók már nem szigetelt, zárt informatikai egységek, hanem dinamikus, hálózatba kapcsolt eszközök, amelyek folyamatosan kommunikálnak a gyártói háttérrendszerrel, felhőszolgáltatásokkal, biztosítói rendszerekkel, illetve különféle külső szolgáltatókkal

[196], [197]. Ebben az ökoszisztémában a kommunikációs protokollok kiválasztása meghatározza a teljes rendszer biztonsági és adatvédelmi szintjét.

A szakirodalom egyértelműen rámutat arra, hogy a HTTP/HTTPS, MQTT és CoAP protokollok a legelterjedtebbek a személygépjárművek internetes, OTA (over-the-air) vagy telematikai kommunikációjában [198], [199], [200]. Ezek a protokollok az alkalmazási rétegben helyezkednek el, amely az információbiztonsági és adatvédelmi problémák szempontjából a legkritikusabb, mivel ezen a szinten történik a felhasználói adatok, vezérlési parancsok és érzékeny járműinformációk továbbítása [201]. A Bosch Automotive Handbook és több átfogó tanulmány is kiemeli, hogy mindhárom protokoll nélkülözhetetlen eleme a modern connected car architektúráknak [202], [203].

A HTTP/HTTPS szabványos, univerzális protokoll, amelyet elsősorban API-hívásokra, OTA szoftverfrissítésekre, valamint webes szolgáltatások elérésére használnak a hálózatra kapcsolt járművek. Az MQTT egy könnyű, publish-subscribe architektúrájú protokoll, amely a telemetriai adatok, eseményüzenetek, diagnosztikai információk továbbításának elsődleges eszköze – különösen ott, ahol erőforrás-korlátozott eszközök, szenzorok és gateway-ek kommunikálnak a háttérrendszerrel vagy egymással [199], [203]. A CoAP pedig az IoT-környezetekre optimalizált RESTful protokoll, amely a gépi kommunikáció és az alacsony sávszélességű, nagy megbízhatóságú adatátvitel igényeit szolgálja ki, egyre több autóipari szenzorrendszerben [204], [205].

Közös jellemzőjük, hogy jelentős IoT és embedded penetrációval bírnak; a járműipar mellett szinte minden modern ipari, egészségügyi vagy okosvárosi megoldásban is megtalálhatók [206]. Mindhárom protokoll támogat valamilyen szintű titkosítást (TLS, DTLS), de a gyakorlati implementációkban ezek a védelmek sokszor hiányosak, nem megfelelően konfiguráltak, vagy teljesen hiányoznak [207], [208]. Ez különösen veszélyessé teszi őket a járművek világában, ahol az adatbiztonsági incidens akár emberéletet is veszélyeztethet [209].

Számos nemzetközi kutatás és szakirodalmi áttekintés is hangsúlyozza, hogy épp ez a három protokoll a legérzékenyebb a biztonsági réseket, konfigurációs hibákat, valamint a rejtett csatornák (covert channels) kialakulását illetően [200], [203], [209], [210]. Velinov és munkatársai részletesen elemzik az OTA kommunikációban megjelenő protokollok támadhatóságát [209], Kim és társai pedig a CoAP és MQTT sérülékenységeit, köztük a nem megfelelő hitelesítés és titkosítás problémáját mutatják

be [201], [210]. Ghafir 2023-as cikke pedig rámutat, hogy az MQTT a leggyakrabban célzott alkalmazási rétegbeli támadási felület az IoT-alapú járművekben [211], [210].

Mindezek alapján indokolt, hogy a disszertáció részletes elemzése a HTTP/HTTPS, MQTT és CoAP protokollokra koncentráljon. Ezek vizsgálata nem csupán a jelenleg elérhető járműkommunikációs technológiák biztonsági szintjének felmérését teszi lehetővé, hanem általános tanulságokkal is szolgálhat a jövőbeli, biztonságosabb autóipari megoldások fejlesztéséhez.

5.3. Protokollok részletes elemzése a STRIDE módszertan mentén

A modern internetkapcsolatra képes járművek hálózati biztonságának vizsgálata során kulcsfontosságú a kommunikációs protokollok fenyegetettségi profiljának feltérképezése. Ehhez a disszertáció a STRIDE módszertant alkalmazza, amely lehetővé teszi a főbb támadási vektorok (azonosságmeghamisítás, manipuláció, letagadhatóság, információszivárgás, szolgáltatásmegtagadás és jogosultságkiterjesztés) rendszerszintű értékelését [99], [211]. A következőkben a három legfontosabb alkalmazási rétegbeli protokoll, a CoAP, az MQTT és a HTTP/HTTPS részletes elemzését mutatom be a STRIDE szempontok, illetve az általános biztonsági és adatvédelmi kihívások mentén.

A CoAP egy kifejezetten erőforrás-korlátozott IoT-rendszerekre tervezett, RESTful elvű protokoll, amely UDP-alapon működik, és különösen alkalmas szenzoradatok, parancsok, illetve állapotinformációk hatékony, kis késleltetésű továbbítására [198], [204]. A járműiparban elsősorban szenzorhálózatok, gateway-ek és felhőalapú szolgáltatások között alkalmazzák.

A STRIDE módszertan alapján a CoAP különösen sérülékeny azonosságmeghamisításra (spoofing) és információszivárgásra (information disclosure), mivel natívan nem biztosít hitelesítést, és a titkosítás (DTLS) sokszor csak opcionális vagy helytelenül konfigurált [201]. A manipuláció (tampering) főként a fejlécek és payload módosításán keresztül, míg a szolgáltatásmegtagadás (DoS) támadások az UDP multicast jellege miatt könnyen kivitelezhetőek. Az üzenetek időzítésén vagy strukturált tokeneken alapuló rejtett csatornák (covert channels) is reális fenyegetést jelentenek [200], [201]. Privacy szempontból a CoAP forgalom jelentős mennyiségű metaadatot és – megfelelő védelem hiányában – akár azonosítható felhasználói vagy járműparamétereket is tartalmazhat, különösen ha az üzenetek nincsenek titkosítva vagy pszeudonimizálva [7]. A CoAP protokoll esetében rejtett csatornák kialakítása több szinten is lehetséges, például időzítési

vagy token alapú technikákkal, illetve a payload struktúrájának manipulálásával [5], [6], [205].

Az MQTT egy rendkívül elterjedt, publish-subscribe architektúrájú üzenetközvetítő protokoll, amely tipikusan TCP-alapon működik, és ideálisan alkalmas telemetriai adatok, állapotváltozások vagy eseményüzenetek továbbítására jármű és backend rendszerek között [199], [201], [203].

A STRIDE szempontú elemzés során azonosságmeghamisítás kockázata emelkedett, mivel a hitelesítés sok implementációban csak jelszavas, vagy akár teljesen hiányozhat; a brute-force támadások, jogosulatlan hozzáférések, valamint a publikus topikok jelentik a fő gyenge pontokat [207], [201]. Manipuláció szempontjából a nem titkosított MQTT-forgalom, illetve a payload mezők közvetlen módosíthatósága sebezhetőséget okoznak. Az információszivárgás veszélye igen jelentős, mivel az MQTT-ben nincsenek beépített titkosítási követelmények; ha nem használják a TLS-t, minden átmenő üzenet szabadon lehallgatható [203], [206]. Letagadhatóság szempontjából a naplózás hiánya vagy hiányossága (audit trail) problémát jelent, különösen, ha az üzenetek nem tartalmaznak egyértelmű forrásazonosítót vagy időbélyeget [208]. DoS támadások kivitelezhetők túlterheléses, illetve bróker-ellenes támadásokkal is, a single point of failure kockázat rendszertervezési sajátosság [177], [201]. Az MQTT-ben különösen egyszerű rejtett csatornákat kialakítani, például a topik nevében, QoS szintekben, session azonosítókban vagy a retained üzenetekben elrejtett adatok révén [204], [205]. Privacy szempontból mind a metaadatok (ki, mikor, melyik topikra küldött üzenetet), mind az üzenetek tartalma érzékeny lehet; az üzenetszintű azonosítás vagy profilozás megfelelő védelem nélkül reális veszélyt jelent [206].

A HTTP/HTTPS protokoll a legáltalánosabban használt webes kommunikációs szabvány, amely az autóiparban is megkerülhetetlenné vált, legyen szó OTA frissítések letöltéséről, API-hívásokról vagy különféle külső szolgáltatások integrációjáról [207]. A STRIDE elemzés szempontjából a titkosítás nélküli HTTP forgalom miatt kiemelkedő az információszivárgás és manipuláció veszélye; a TLS (HTTPS) használata esetén a tanúsítványok kezelése, a CA láncok helyes menedzsmentje és a végpont-azonosítás szintén kritikus biztonsági tényező [208]. Az azonosságmeghamisítás itt leggyakrabban az API végpontok elégtelen autentikációjából fakad, míg a letagadhatóságot a nem megfelelő naplózás, session kezelési hibák, vagy cookie-kon keresztül végzett támadások

veszélyeztethetik [207], [208]. A HTTP/HTTPS protokollokban is léteznek rejtett csatornák, például a header mezőkben, az URI struktúrában, a cookie-kban, vagy az üzenetek időzítésében [209]. Privacy szempontból különösen kritikus a session management, az API naplózás, valamint a megfelelés adatvédelmi szabályozásoknak (például GDPR); nem megfelelő implementáció esetén jelentős kockázatot jelenthet a személyes adatok szivárgása vagy a felhasználói profilok visszafejtése [208], [210].

Mindhárom protokoll esetében kimutatható, hogy a STRIDE-módszertan minden fenyegetéstípusára léteznek konkrét példák (4. táblázat). Az, hogy ezek a támadási lehetőségek a gyakorlatban mennyire jelentős kockázatot jelentenek, elsősorban az implementáció minőségétől, a titkosítás helyes alkalmazásától, a hozzáférés-szabályozás megvalósításától és a naplózási mechanizmusok színvonalától függ az adott járműkommunikációs környezetben. Az irodalom egyértelműen alátámasztja, hogy ezek a protokollok napjainkban a legkritikusabb pontok az autóipari adatforgalom védelmében [197], [198], [207], [208].

STRIDE kategória	CoAP	MQTT	HTTP/HTTPS
Spoofing (azonosságmeghamisítás)	Nincs natív hitelesítés, token hamisítható	Hitelesítés gyakran hiányzik vagy gyenge	API kulcsok vagy session azonosítók ellophatók
Tampering (manipuláció)	Üzenet vagy header módosítása DTLS hiányában lehetséges	Payload vagy topic manipulálható titkosítás nélkül	Request/response módosítás titkosítás nélkül lehetséges
Repudiation (letagadhatóság)	Nincs naplózás, az üzenet forrása letagadható	Nincs audit trail vagy időbélyeg az üzeneteknél	API hívások vagy műveletek logolásának hiánya
Information Disclosure (információszivárgás)	Titkosítás nélkül metaadatok és payload szivárog	Nem titkosított üzenetekben érzékeny adatok szivároghatnak	HTTP forgalomban credentials vagy személyes adatok szivárognak
Denial of Service (szolgáltatásmegtagadás)	UDP flood vagy multicastinggal leterhelhető	Bróker túlterhelése, session flood támadás	HTTP endpoint túlterhelhető (DoS támadás)
Elevation of Privilege (jogosultságkiterjesztés)	Jogosultságkezelés hiánya vagy hibája miatt emelt jog érhető el	Jogosulatlan hozzáférés a topikokhoz lehetséges	Hibás access control, privilegizált API-k elérése

4. táblázat - STRIDE módszertan szerinti elemzés. Forrás: saját forrás.

5.4. Következtetések

A fejezetben elvégzett részletes elemzés alapján világossá vált, hogy az internetkapcsolattal rendelkező járművekben alkalmazott kommunikációs protokollok – különösen a CoAP, MQTT és HTTP/HTTPS – már alapvető működésükből fakadóan is lehetőséget kínálnak rejtett csatornák kialakítására. Ezek a protokollok a járműkommunikáció sajátos funkcionális elvárásai, például az alacsony késleltetés és az erőforrás-takarékosság miatt, gyakran kompromisszumokat kötnek a biztonsági mechanizmusok teljeskörű alkalmazásában. Az elemzett példákból látható, hogy a rejtett csatornák kialakítására több technikai lehetőség is nyílik – akár fejlécmezők, metaadatok, időzítés vagy payload-manipuláció révén –, és ezek a technikák sok esetben a protokoll szabványos működésével összefonódva jelennek meg.

A vizsgálat azt is megmutatta, hogy a klasszikus technikai biztonsági intézkedések, mint például a titkosítás, a hitelesítés vagy a hozzáférés-vezérlés, bár képesek csökkenteni bizonyos típusú támadások sikerességét, önmagukban nem elegendőek a rejtett csatornák teljes körű megszüntetésére vagy megbízható detektálására. A rejtett csatornák az adott kommunikációs protokoll normál működésének részeként, nehezen elkülöníthető módon jelennek meg, ezért hagyományos kontrollokkal csak részben szűrhetők ki.

A bemutatott elemzési folyamat eredményeképpen megfogalmazható az alábbi tézis (T4): Az internetkapcsolattal rendelkező járművek kommunikációs protokolljai – funkcionális követelményeik (pl. alacsony késleltetés, korlátozott erőforrás-használat) miatt – alkalmasak rejtett csatornák létrehozására, amelyek technikai védelmi eszközökkel, például titkosítással, nem szüntethetők meg teljes mértékben. Ezért a rejtett csatornák azonosítása és célzott védelmi intézkedések kidolgozása elengedhetetlen a járműkommunikáció biztonságának fenntartásához. Ez a tézis alapot ad a további kutatási és fejlesztési irányok kijelöléséhez, különösen a járműipari kommunikációs rendszerek új generációs védelmi stratégiáinak kialakításában.

6. AZ ADATKÜLDÉS MENNYISÉGI MODELLEZÉSE ÉS ELEMZÉSE

A(z) „Adattovábbítási modellezés és szimuláció” című kutatási szakasz célja annak vizsgálata volt, hogy milyen módon használhatók fel az internetkapcsolattal rendelkező járművek szenzor- és kommunikációs adatai kijelölt objektumok vagy célszemélyek rejtett megfigyelésére, és ez milyen nemzetbiztonsági kockázatokat hordoz flottaszinten?

Az 5. kutatási kérdésre adott válaszkeresés megalapozta az elemzési irányokat, és hozzájárult a vizsgálat struktúrájának kialakításához.

A jelen fejezet célja ezen rejtett csatornák kapacitásának becslése: mennyiségi modellt dolgoztam ki különféle szituációkra, figyelembe véve az egyszerű szenzoradatokat, valamint a fejlett szoftveres funkciók (pl. kameraképek, járműdiagnosztikai információk) adatforgalmát. A vizsgálat során választ kerestem arra, hogy mekkora sávszélességű adat továbbítható rejtetten egyetlen kompromittált járműből, illetve milyen mértékű lehet a potenciális adattovábbítás egy teljes autóflotta esetében. A modellezés rámutatott arra, hogy a nagyfelbontású szenzoradatok és a fejlett vezetéstámogató rendszerek lehetőséget biztosíthatnak akár célzott észrevétlen megfigyelési műveletek támogatására is.

A fenti példák és a kvantitatív modell eredményei megerősítik, hogy a járművek kiberbiztonsági kockázatai nem csupán technikai kérdések, hanem nemzetbiztonsági relevanciával is bírnak. A decentralizált architektúrák, az eltérő szabványértelmezések, valamint a gyártók és beszállítók eltérő gyakorlatai lehetőséget teremtenek arra, hogy az egyes járművek – vagy akár egész járműflották – tudtukon kívül információszerzésre használhatók legyenek.

Az elvégzett becslések alapján elmondható, hogy az internetre kapcsolt, fejlett fedélzeti rendszerekkel rendelkező járművek rejtett csatornákon keresztül napi több megabájt érzékeny adat továbbítására lehetnek képesek úgy, hogy ezt sem a felhasználó, sem a gyártó nem észleli időben. Flottaszinten ez olyan volumenű adatmozgást jelenthet, amely célzott támadási szcenáriókban kritikus nemzetbiztonsági kockázatot jelenthet, különösen érzékeny objektumok, iparágak vagy személyek megfigyelése esetén.

Bár egyes források szerint a járműkommunikáció nem minden esetben titkosított, ezt tudományosan még nem igazolták egyértelműen. A tanulmány ezért a titkosított adatkezelést tekinti alapértelmezettnek, ugyanakkor rámutat arra, hogy a végponti kompromittáció – ahol az adatok titkosítatlanul is hozzáférhetők – komoly biztonsági kockázatot jelent. Mindez azt jelenti, hogy az adatvédelem nem merülhet ki pusztán a titkosítás alkalmazásában.

Ahogyan a korábbi fejezetekben és publikációimban bemutattam, a személygépjármű mint összetett termék bonyolultsága miatt az információbiztonsági intézkedések alapvető kockázatelemzésének végrehajtása különösen nehéz [212]. 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.

A téma érzékenysége miatt a rendelkezésre álló adatok nem nyújtanak teljes körű és részletes képet az internetkapcsolattal rendelkező személygépjárművek adatátviteli mechanizmusairól. Ugyanakkor különböző független adatvédelmi szervezetek és kutatóintézetek értékes forrásokat biztosítanak a témakör jobb megértéséhez. Caltrider és munkatársai [213] a modern járművekben zajló adatgyűjtési gyakorlatokat vizsgálták, különös figyelmet fordítva az adatkezelési folyamatok átláthatóságára és az ezekből fakadó adatvédelmi kockázatokra. A jelentés, amely a Mozilla Foundation „Privacy Not Included" projektje keretében készült, átfogó képet ad arról, hogy a mai okosjárművek milyen típusú adatokat gyűjtenek – többek között helymeghatározási információkat, vezetési szokásokra vonatkozó adatokat, valamint az infotainment rendszerek használatával kapcsolatos interakciókat.

A vizsgálat rámutatott, hogy az adatok gyűjtése több forrásból történik: szenzorokból, GPS-rendszerekből, kamerákból és fedélzeti számítógépekből, majd ezek az információk jellemzően az autógyártók szervereire vagy harmadik fél szolgáltatóihoz kerülnek továbbításra. A kutatás kiemeli, hogy az adatvédelmi szabályzatok gyakran nem tesznek egyértelmű nyilatkozatot arról, pontosan milyen adatokat gyűjtenek, milyen célokra használják azokat fel, illetve kikkel osztják meg. Ezen adatok kezelése tehát nem kizárólag a jármű technikai rendszereitől függ, hanem attól is, milyen módon biztosítják az adatáramlás szabályozását, naplózását és ellenőrzését.

Az elérhető kutatások alapján egyértelműen megállapítható, hogy az internetkapcsolattal rendelkező személygépjárművek adattovábbításával kapcsolatos aggályok számos korábbi tanulmányban is megjelentek. Több adatforrás – különösen a jármű által gyűjtött szenzor- és telemetriai adatok – biztonsági kockázatot hordozhat, amelyre már számos lehetséges válasz is született, köztük meglehetősen drasztikus javaslatok is (például egyes autótípusok forgalomból történő kivonása).

Mindazonáltal a rendelkezésre álló szakirodalomban jelenleg hiányoznak azok az empirikus alapú számítások vagy modellezések, amelyek kvantitatív módon becsülnék meg, hogy a különböző típusú adattovábbítások mekkora biztonsági kockázatot

hordoznak, illetve hogy egy adott csatorna milyen mennyiségű érzékeny információ továbbítására lehet alkalmas.

6.1. Adattovábbítás

A következő fejezet célkitűzése az, hogy kvantitatív modellezés segítségével megbecsülje a személygépjárművek által használható rejtett kommunikációs csatornák adattovábbítási képességét, különös tekintettel a támadó potenciális céljaira.

A vizsgálat célja annak feltárása, hogy milyen típusú és mennyiségű adat továbbítható egy kompromittált rendszerből, és hogy ez az adatmennyiség milyen típusú visszaélésekre lehet elegendő – akár egyedi járművek, akár járműflották szintjén értelmezve. 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.

Egy ABS (blokkolásgátló rendszer) vezérlőegység (ECU) pl. A Bendix Gen 4 és Gen 5 ABS rendszerek esetében az ECU másodpercenként 100-szor frissíti a nyomásszabályozó szelepek vezérlését [214], Az ABS modulátor másodpercenként akár 15-ször is pulzálhatja a féknyomást [215]. ESP (elektronikus stabilitásprogram) vezérlőegység, pl. a Bosch ESP rendszer vezérlőegysége másodpercenként 25-ször [216] hasonlítja össze a jármű tényleges mozgását a kívánt irányával. Nem publikált adat, hogy ezeket az adatokat hol tárolja az autó, viszont tudjuk hogy számos autónál ezeket az adatokat meg kell osztani egy távoli adatközponttal. Kutatásom során azzal a feltételezéssel éltem, hogy ezen nagyságrendű adatok esetén reális azt feltételeznünk hogy a kompromittált személygépjármű másodpercenként egy rejtett adatot képes elküldeni. Mindez azt jelenti hogy a pár száz másodpercenkénti szenzoradatból mindössze egy hordoz rejtett információt, amely reális lehet a kockázatokat figyelmbe véve.

Ha egy autó típusról kiderül, hogy bizonyíthatóan rejtett adatok küld, akkor a piaci kár felbecsülhetetlen a gyártó számára. Egy ilyen rejtett csatorna esetén a támadónak nagyon kis hatásfokú adatküldést kell alkalmaznia, hogy elkerülje a kompromittációt. Mindezek miatt döntöttem a konzervatív egy byte/másodperc becslésnél, amely azt is jelenti hogy valójában ez az adatküldésnek egy becsült alsó határa.

Mindezek miatt az említett adatátviteli sebességgel közel 3 402 000 másodpercre (körülbelül 39,375 napra) lenne szükség ennek az adatmennyiségnek (egy darab 900x1260 képpontos tömörítetlen kép) a továbbítására. A 5. táblázatban összefoglaltam az adatátviteli sebességeket.

Adattípus	Átlagos adatgenerálás
Radar	10–100 KB/s (~1–8 GB/nap)
LiDAR	10–70 MB/s (~800 MB – 6 TB/nap)
Kamerák	20–50 MB/s (~1–4 TB/nap)
Ultrahangos érzékelők	10–50 KB/s
Fék/ABS/ESP szenzorok	kB/s (pár MB/nap)
Motor/Fogyasztás/Telemetria	1–10 MB/nap
GPS	1–5 MB/nap

5. táblázat - Személygépjárművek által generált adatok átviteli becslése. Forrás: saját forrás.

A bemutatott becslések alapján megállapítható, hogy a modern személygépjárművek – különösen az önvezető funkciókkal vagy fejlett szenzortechnikával felszerelt modellek – jelentős mennyiségű adatot képesek generálni és potenciálisan kiszivárogtatni. Ezen adatmennyiségek – különösen kameraképek, LiDAR- és GPS-adatok esetében – lehetővé teszik akár egyéni felhasználók, akár kritikus objektumok megfigyelését és a róla szóló adatok rejtett eljuttatását egy külső támadó felé. Ez a típusú adatszivárgás technikai védelmi eszközökkel nem mindig küszöbölhető ki, és a jelenlegi szabályozási és gyártói kontrollmechanizmusok nem képesek kellően átfogó védelmet nyújtani a fenyegetéssel szemben. A kutatás tehát rámutat: a személygépjárművek által generált és továbbított adatok rejtett csatornákon való kivezetése valós és számszerűsíthető kockázatot jelent, amelyre sem a szabványosítás, sem a jelenlegi kiberbiztonsági keretrendszerek nem nyújtanak teljes körű megoldást.

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) [217].

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 [218] 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.

6.1.1. 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 a klasszikus 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 elektronikus járművezérlő egységek (ECU-k) működésének frekvenciája és adatgenerálása alapján becslések készíthetők a potenciálisan továbbítható rejtett adatmennyiségekre. Például a Bendix Gen 4 és Gen 5 típusú blokkolásgátló rendszerek

(ABS) vezérlőegységei másodpercenként akár 100 alkalommal frissítik a nyomásszabályozó szelepek vezérlését [214], míg az ABS modulátor egyes rendszerekben akár másodpercenként 15-ször is képes pulzált féknyomásvezérlésre [215]. Az elektronikus stabilitásprogram (ESP) esetében a Bosch ESP rendszere például másodpercenként 25-ször végzi el a jármű tényleges mozgásának összevetését a kívánt haladási iránnyal [216].

A rendelkezésre álló források nem tartalmaznak egyértelmű információt arra vonatkozóan, hogy e vezérlőegységek által generált adatok fizikailag hol kerülnek tárolásra a járművön belül, azonban ismert, hogy több gyártó esetében ezen adatok továbbítása egy központi, akár távoli adatfeldolgozó egység felé is megtörténhet. Vizsgálatom során konzervatív becsléssel éltem, amely szerint – figyelembe véve a szenzoradatok gyakoriságát, az adatküldési mechanizmusok biztonsági sajátosságait, valamint a támadók észlelésének elkerülését célzó kockázatminimalizálási stratégiákat – életszerűnek tekinthető, hogy egy kompromittált személygépjármű másodpercenként legfeljebb egy darab rejtett adatot továbbítson titkos kommunikációs csatornán keresztül. Ez azt jelenti, hogy a másodpercenként keletkező több száz szenzoradat közül mindössze egy válik a rejtett csatorna részévé – ami erősen csökkenti a felfedezhetőség kockázatát, miközben mégis lehetővé teszi érzékeny adatok szivárogtatását.

E konzervatív becslés alapján, egy byte/másodperc sávszélességgel számolva, egy tömörítetlen, 900×1260 képpontos kép továbbításához – amely körülbelül 3,4 MB adatot jelent – mintegy 3 402 000 másodperc, azaz közel 39,4 nap folyamatos adatküldésre lenne szükség. Ez a számítás nemcsak érzékelteti a rejtett csatornák adatátviteli kapacitásának fizikai korlátait, hanem azt is alátámasztja, hogy a támadó számára a tartós, észrevétlen jelenlét jelentheti a legfőbb előnyt. E megközelítés alátámasztja az 5. tézis megállapítását, miszerint még minimális sávszélességű rejtett csatornák is komoly adatvédelmi és nemzetbiztonsági kockázatot jelenthetnek, különösen akkor, ha a kompromittált járművek nem egyedileg, hanem flottaszinten működnek.

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 [219], [220]. 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. Az ilyen típusú szolgáltatások nagyobb mennyiségű adatok folyamatosabb továbbítását igénylik. Mindezekhez 1kB/másodperc adattovábbítást feltételeztem. A rejtett adatok arányához az előzőekben alkalmazott “óvatos” feltételezéssel éltem, amely azt eredményezte, hogy 4 adategységet vettem figyelembe másodpercenként. Ez az érték azt jelenti, hogy egy képet egy nap alatt lehet továbbítani rejtett csatornán keresztül, ha azt ezt szolgáló célszoftver kompromittálódott.

A lehetőségeket még tovább bővíti, ha ennél is összetettebb szolgáltatásokról feltételezzük hogy rejtett csatornákat tartalmaznak. Mint korábban említettem, 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 különbséget a 6. táblázat szemlélteti.

	Kép mint bitkép	**90%-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

6. táblázat - A képi adatok rejtett csatornán keresztül történő továbbításának összefoglalása. Forrás: saját forrás.

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.

6.1.2. 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 [221] 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.

Iwakami és munkatársai tanulmánya [222] 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 [222], [223], 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 beszéd mintát 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 [224] azt mutatták, hogy mindössze 5 másodpercnyi hangfelvétel elegendő valaki hangjának lemásolásához (voice cloning). 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. A különbséget a 7. táblázat szemlélteti.

	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

7. táblázat - Hangadatok rejtett csatornán keresztül történő továbbításának összefoglalása. Forrás: saját forrás.

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.

6.1.3. Helyadatok küldése MQTT rejtett csatornákon keresztül

A helymeghatározási adatok továbbítása a legtöbb modern személygépjármű esetében az alapvető működés részét képezi, így gyakran nincs szükség rejtett adatküldési mechanizmusokra e típusú információk célba juttatásához. A fedélzeti navigációs rendszerek általában valós időben jelenítik meg a jármű pontos pozícióját a térképfelületeken, emellett pedig bizonyos működési körülmények között külső szolgáltatók vagy technikai egységek – például gyártói szervizhálózatok – is hozzáférhetnek ezen adatokhoz.

Személyes konzulensi tapasztalat alapján megállapítható, hogy például a Tesla szervizhálózata képes lokalizálni és távolról hozzáférni az adott járműhöz anélkül, hogy a tulajdonos fizikai jelenléte vagy kulcsa szükséges lenne, mindössze egy telefonos megerősítés alapján – feltéve, hogy a jármű nyilvánosan hozzáférhető helyen (pl. utcán) parkol, és rendelkezik aktív internetkapcsolattal. E gyakorlat jól példázza, hogy a járművek földrajzi helyzetének lekérdezése és kezelése technológiailag már jelenleg is adott, a kérdés legfeljebb szabályozási és adatvédelmi szempontból releváns.

Ettől függetlenül érdemes megvizsgálni, hogy milyen technikai lehetőségek állnak rendelkezésre a helyadatok rejtett csatornán keresztül történő továbbítására – különösen olyan esetekben, amikor a gyártó vagy az üzemeltető politikája elviekben tiltja az ilyen típusú adatkommunikációt, vagy amikor a felhasználó az adatmegosztást korlátozó beállításokat alkalmaz.

A helyadatok MQTT protokollon keresztüli rejtett továbbítása, például gyorsulási vagy hőmérsékleti adatnak álcázva, 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 [225] 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, akiket beazonosíthatnak azáltal hogy többször jártak mind a CIA főhadiszállása és az NSA központja közelében). 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.

6.2. Hozzáférés több személygépjármű adataihoz

Ha körülnézünk a sajtóban, könnyen találhatunk arra utaló híreket, hogy személygépjátműveket kihasználva valamilyen szereplő titkos megfigyelést hajt végre. Egy akadémiai áttekintés világossá teszi, hogy az okosjárművek szenzorai és közlekedési adatai katonai és hírszerzési alkalmazások számára is relevánsak lehetnek [226]. Az ENISA által is hivatkozott tanulmányok szerint már több mint húszféle soft-privacy fenyegetés azonosítható az autóiparban [227], beleértve a járművek lokációjának és biometrikus adatainak harmadik fél általi megszerzését. Konkrét példaként említhető a US Commerce Department vizsgálata, mely rámutatott, hogy kínai okosjárművek képesek lehetnek érzékeny információkat továbbítani külföldi szerverekre, ezért az amerikai kormány javasolta ezek kivonását a belső piacról [228], [229]. A biztonsági elemzők ennél is tovább mennek: egy CSIS jelentés szerint nem csak adatgyűjtés zajlik –

elméletileg még a járművek távoli irányításával is kísérletezhetnek ellenséges hatalmak, ami „szabotázs” vagy „tömegösszeomlás” esetén súlyos biztonsági kockázatot jelent [230]. A brit védelmi tanácsadók pedig azt javasolták, hogy tisztségviselők ne csatlakoztassák személyes készülékeiket kínai gyártmányú elektromos járművekhez, mivel azok óriási mennyiségű adatot gyűjthetnek és továbbíthatnak, ami kompromittálhatja a belső bizalmas kommunikációt [231].

Az alábbiakban jellemzett forgatókönyvben feltételezem, hogy a fenyegető szereplőnek több autóhoz is hozzáférése van, és a rendszeres adatkommunikációt használja titkos csatornaként a rosszindulatú tevékenység végrehajtására. Megközelítésemben az személygépjárművet a korábbi fejezetekben bemutatott módon és kapacitással információk továbbítására képesnek feltételezem az adatokat a rendszeres hálózati kommunikációban elrejtve. A több járműhöz és azok adataihoz való hozzáférés egyedülálló lehetőséget biztosít a fenyegetést okozó szereplők számára. Vélelmezem, hogy a fenyegető szereplő hozzáférhet az összes szükséges intelligens járműadathoz, mint például a következőkhöz:

- a jármű GPS koordinátái az időbélyegzőkkel együtt;
- a jármű által belülről és kívülről készített kameraképek, azok időbélyegzőjével együtt;
- a jármű belsejében zajló hangkommunikáció, szintén az időadatokkal együtt.

Azt is figyelembe vesszük, hogy a jármű rendelkezik a következőkkel:

- rendszeres kommunikáció az akkumulátorra vonatkozó naprakész adatok szolgáltatása érdekében;
- rendszeres kommunikáció a szoftverfrissítések ellenőrzésére;
- rendszeres kommunikáció az önvezető adatok megszerzésére és jelentésére;
- rendszeres kommunikáció a gépjármű biztosítóval.

Feltételezésem szerint a fenyegető szereplő képes ezen adatcsatornák egyikét használatba venni és a kommunikációt rejtett csatornaként használni a rosszindulatú tevékenység

elrejtésére. Az alábbiakban tehát azt feltételezem, hogy a járművek egy jelentősebb csoportjához egy külső szereplő hozzáfér, ezáltal lehetősége van egy előre meghatározott algoritmus alapján adatokat lekérni. Ilyen adat lehet pl. az autó külső kameráinak felvételei. Ezek alapján néhány elméleti lehetőséget vizsgálok.

A különböző lehetőségek vizsgálatánál két alapvető jellemzőt figyelembe kell venni:

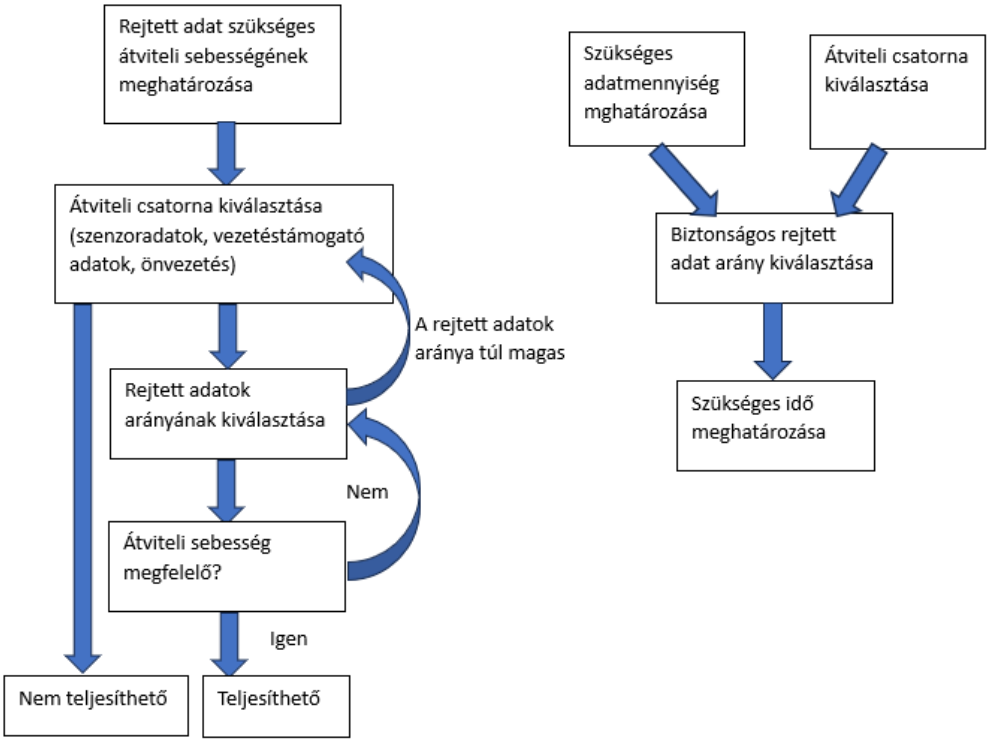
- az algoritmus komplexitása, amit a személygépjárműnek végre kell hajtania a megfigyelő művelet során;
- a többlet adatok mennyisége, amit a személygépjárműnek továbbítania kell a támadó (megfigyelő) felé.
- Mivel a fenti körülményeket vizsgáló, az itt bemutatott elméleti modellhez hasonló leírás a disszertáció írásának időpontjában nem állt rendelkezésre, így a továbbiakban ismertetett információk során az általam kalkulált értékek bemutatására kerül sor.

6.2.1. Kijelölt területek megfigyelése

Egy elméleti lehetőség a kijelölt objektumok környezetének megfigyelése. Egy ilyen jellegű támadásnál a jármű GPS koordináták alapján aktiválja a megfigyelést. Az algoritmus tehát annak aktuális pozícióját figyeli és abban az esetben, ha egy meghatározott pozícióba kerül, fényképeket készít a külső kamerák segítségével. Ezen fényképeket a telekommunikációs hálózaton keresztül képes továbbítani a támadó felé. A támadó algoritmus komplexitása ebben az esetben alacsony.

A modellezés során abból a feltételezésből indultam ki, hogy a támadó célja egy adott mennyiségű rejtett adat átvitele egy előre meghatározott időintervallumon belül. Ezt a problémát úgy közelítettem meg, hogy a kívánt rejtett adatküldési sebességből indultam ki, és vizsgáltam, hogy a támadó milyen lehetőségekkel rendelkezik a rejtett adatforrások és a rejtett adatok arányának megválasztásakor. Nyilvánvaló, hogy minél nagyobb arányban tartalmaz rejtett adatot az adott kommunikációs csatorna, annál nagyobb a lebukás, azaz a csatorna kompromittációjának kockázata. A gyakorlatban ezért a rejtett adatok aránya rendkívül alacsony kell, hogy legyen – különösen érzékeny környezetben, ahol komoly következményekkel járna, ha például egy járműgyártóról kiderülne, hogy titokban adatokat továbbít.

A modell alapján minden paraméterezett esetben kiértékelhető, hogy a kiválasztott (vagy megkövetelt) rejtett adatküldési sebesség elérhető-e. Ha nem, két irányban kereshető megoldás: vagy növeljük – egy ésszerű, lebukási kockázattal még elfogadható – szintig a rejtett adatok arányát, vagy alternatív, nagyobb sávszélességű csatornát választunk. Amennyiben egyik lehetőség sem vezet eredményre (például nincs elérhető nagyobb sávszélességű csatorna), a modell az adott paraméterek mellett „nem teljesíthető" állapotot eredményez. A folyamatot a 9. ábra szemlélteti.



9. ábra - A rejtett adatok továbbításához szükséges átviteli sebesség megállapítása és a csatorna kiválasztása. Forrás: saját forrás.

A rejtett funkciók az alábbi elemeket tartalmazzák:

- folyamatos helypozíció figyelés, adott pozíciókban az extra funkciók aktiválása és deaktiválása;
- aktivált állapotban fényképek készítése;
- az elkészített képek azonnali vagy késleltetett rejtett továbbítása.

Az általam alkalmazott modell a kontrollált autók számából mint bemenő adat és a forgalom nagyságából kiindulva vizsgálja a támadó lehetőségeit. Vizsgálatomhoz egy Budapest nagyságú várost feltételeztünk 500.000 autóval. Az autók eloszlása a városban

nem egyenletes, illetve a gépjármű tulajdonosának lakhelye, munkahelye és egyéb életvitelszerű mozgása befolyásolja az autó lehetőségeit.

A modell felépítésekor a városi forgalomban közlekedő járművek elhaladását egy adott objektum (például épület vagy személy) előtt a szakirodalomban széles körben használt Poisson-folyamattal közelítjük[105], [106], [107]. Ez az elméleti keret abból indul ki, hogy az események – jelen esetben az autók elhaladása a célpont előtt – egymástól függetlenek, és az átlagos gyakoriságuk (jelölése λ, például autók/perc) ismert vagy becsülhető.

A mozgó autóflották eloszlását, városi mozgását ehhez kapcsolódóan egyszerűsített random waypoint modellel reprezentáljuk[106], amelyben a járművek véletlenszerű pontok között mozognak, így hosszú távon az elhaladások időbeli eloszlása jól közelíthető a Poisson-folyamat paramétereivel. A random waypoint elmélet szerint, ha elegendő számú autó közlekedik a városban véletlenszerűen, akkor a célterületen az elhaladások száma statisztikailag Poisson-eloszlást követ. (A Possion-folyamat számítását a 9. Mellékletben foglaltam össze.)

Ez a modell jól validált a mobil szenzorhálózati szakirodalomban[105][106][107], ahol azt is kimutatták, hogy viszonylag kis számú mozgó szenzor is jelentős lefedettséget és rendszeres megfigyelést tud biztosítani.

Mindezektől függetlenül egyszerűsített módon azt feltételeztük, a városban lévő autók egyenletesen járják a várost. További feltételezéseink a megfigyelt épülettel kapcsolatosak. Az elkészített vizsgálatunkban azt feltételezzük hogy a megfigyelt épületben emberek dolgoznak vagy laknak. Egy ember legalább napi 4 percet az épületen kívül, de az épület környezetében van, az okos autók által vizuálisan elérhető területen (2 perc érkezéskor, 2 perc távozáskor) azaz maximum annak 10 méteres körzetében.

A forgalom nagyságát percenkénti áthaladó autószámmal vesszük figyelembe. Egy egysávos úton 50-es tempóval 10 autó halad át percenként egy sávban. Az autók száma természetesen függ a napszaktól, a sávok számától és az esetleges közlekedési dugóktól, lámpáktól és a megengedett sebességtől. A vizsgálatunk másik bemenő paramétere a kontrollált autók száma. Megvizsgáltuk a lehetőséget azokban az esetekben ha a támadó 1, 100, 1000, 10.000 illetve 100.000 gépjármű adataihoz fér hozzá (8. tábázat):

autók száma melyekhez a támadó hozzáfér	5 gépjármű percenként / napi 5000	10 gépjármű percenként / napi 10000	20 gépjármű percenként / napi 20000	40 gépjármű percenként / napi 40000
1 gépjármű	kb. évente 2 fotó	kb. 3 havonta egy fotó	kb. havonta egy fotó	kb. 2 hetente 1 fotó
100 gépjármű	kb. naponta egy fotó	kb. naponta 2 fotó	kb. 4 óránként egy fotó	kb. 2 óránként egy fotó
1000 gépjármű	kb. 2 óránként egy fotó	kb. óránként egy fotó	kb. fél óránként egy fotó	kb. 15 percenként egy fotó
10000 gépjármű	10 percenként egy fotó	5 percenként 1 fotó	2-3 percenként egy fotó	1-2 percenként egy fotó/teljes megfigyelés

8. táblázat - Kijelölt személy megfigyelésének hatékonysága kompromittált járműflották részvételével. Forrás: saját forrás.

Ez a táblázat modellezi, hogy mekkora gyakorisággal lehet képalapú információt (például az utastérből vagy a környezetből származó fényképeket) továbbítani rejtett csatornákon keresztül, különböző méretű, kompromittált járműflották esetén. A modell alapját az a feltételezés képezi, hogy egyetlen jármű rejtett csatornán keresztül percenként 5–40 KB adatot képes továbbítani (ennek megfelelően napi 5 000–40 000 bájtnyi információ), amely megfelelő tömörítéssel lehetővé tehet például egy-egy fénykép továbbítását. A táblázat szemlélteti, hogy míg egyetlen kompromittált jármű esetén csupán havi vagy negyedéves szinten lehet rejtetten képi adatot továbbítani, addig nagyobb méretű – 10 000 vagy 100 000 járműből álló – kontrollált flotta már lehetőséget biztosít gyakorlatilag valós idejű, folyamatos megfigyelésre. A sávszélesség halmozódása révén a támadó jelentős mennyiségű vizuális információhoz juthat hozzá, amely nem csupán adatvédelmi, hanem akár nemzetbiztonsági kockázatokat is felvet. A modell tehát alátámasztja az 5. tézis megállapítását, miszerint az aggregált adatszivárgás volumene flotta szinten kritikus megfigyelési kapacitást biztosíthat egy támadó számára.

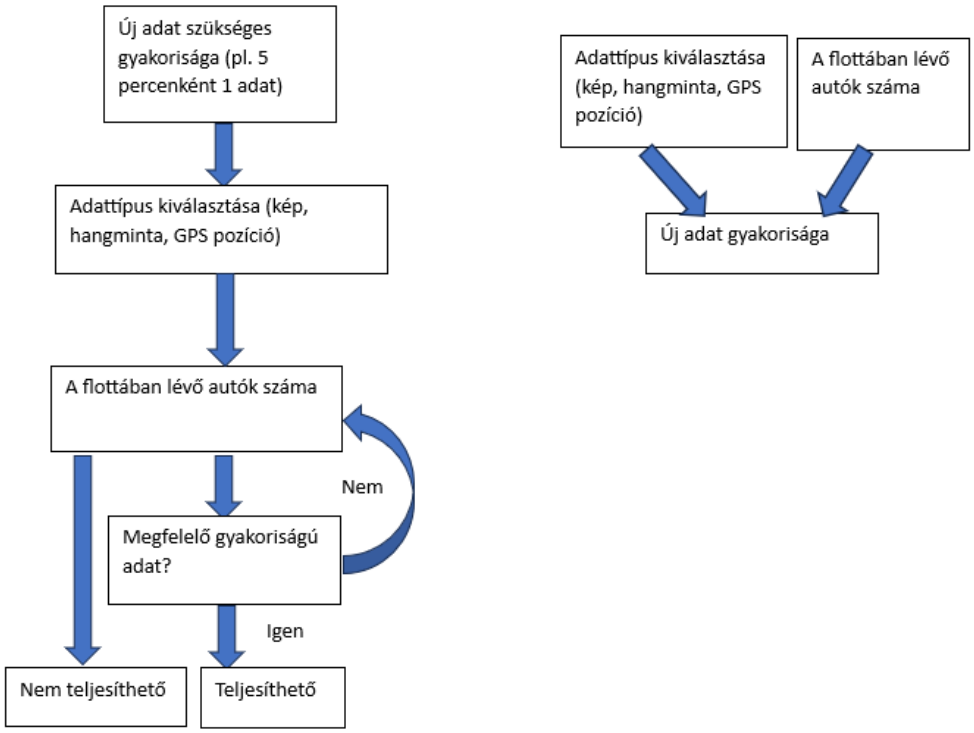
6.2.2. Kijelölt személyek megfigyelése

A kijelölt személy megfigyeléshez tartozó algoritmus komplexitása ebben az esetben lényegesen magasabb. Ebben az esetben a gépjárműnek folyamatos arcfelismerést kell végeznie a kamerák képeiből. A rejtett funkciók az alábbi elemeket tartalmazzák:

- folyamatos arcfelismerés a vizuálisan elérhető személyekre, adott személy beazonosítása esetén a további szükséges funkciók aktiválása;

- aktivált állapotban fényképek tárolása és a GPS adatok lementése;
- az elkészített képek és GPS adatok azonnali vagy késleltetett rejtett továbbítása;
- a kijelölt személy megfigyeléséhez azt feltételezzük hogy a célszemély napi 20 perc és 2 óra közötti időtartományt tartózkodik az utcán, az okos gépjárművek által vizuálisan elérhető területen.

A 10. ábrán az időtényezőt külön választva azt vizsgáltam, hogy egy adott csatorna esetén, előre rögzített teljes adatmennyiség mellett, mennyi idő szükséges a kívánt rejtett adatmennyiség átviteléhez, amennyiben konzervatív becsléssel a teljes adatforgalom 1%-a használható rejtett adatként. Ez a megközelítés különösen indokolt, mivel a detektálás kockázata jelentős mértékben nő a rejtett adatok arányának növelésével. Az elemzés eredményei a mellékelt táblázatokban is megtalálhatók, ahol a különböző csatornák és paraméterek mellett részletesen látható, hogy az egyes konfigurációk milyen időigény mellett teszik lehetővé a kitűzött rejtett adat átvitelét.



10. ábra – Szükséges adatküldési gyakoriság megállapítása, adattípus kiválasztása. Forrás: saját forrás..

A 9. táblázat szemlélteti, hogy a megfigyelési sűrűség miként skálázható az utcai jelenlét és a kompromittált járművek száma függvényében.

autók száma melyekhez a támadó hozzáfér	napi 20 perc forgalomban	napi 40 perc forgalomban	napi 1 óra forgalomban	napi 2 óra forgalomban
1 gépjármű	kb. 100 naponta egy detektált pozíció	kb. 50 naponta egy detektált pozíció	kb. 20-30 naponta egy detektált pozíció	kb. 10-20 naponta egy detektált pozíció
100 gépjármű	kb. naponta egy detektált pozíció	kb. naponta 2 detektált pozíció	kb. naponta 3 detektált pozíció	kb. naponta 6-8 detektált pozíció
1000 gépjármű	kb.naponta 10 detektált pozíció	kb.naponta 20 detektált pozíció	teljes megfigyelés	teljes megfigyelés
10000 gépjármű	teljes megfigyelés	teljes megfigyelés	teljes megfigyelés	teljes megfigyelés
100000 gépjármű	teljes megfigyelés	teljes megfigyelés	teljes megfigyelés	teljes megfigyelés

9. táblázat - Kijelölt személy megfigyelésének hatékonysága kompromittált járműflották részvételével, a forgalomban töltött idő függvényében. Forrás: saját forrás.

A fenti eredmények alapján megállapítható, hogy már viszonylag kis számú kompromittált jármű is lehetővé teszi egy kijelölt személy periodikus követését, amennyiben a célpont rendszeresen tartózkodik nyílt, vizuálisan elérhető közterületen. A járműflotta méretének növekedésével a megfigyelés gyakorlatilag folyamatossá válik („teljes megfigyelés”), amely új szintre emeli a magánszféra sérelmének lehetőségét, és stratégiai kockázatot jelenthet kiemelt célpontok esetén. Ez a modell tovább erősíti az 5. kutatási kérdés relevanciáját, miszerint a gépjárműflották – megfelelő rejtett csatornák és képfeldolgozó algoritmusok birtokában – potenciálisan hatékony eszközeivé válhatnak célzott, akár államilag vagy szervezetten végrehajtott megfigyelési műveleteknek.

6.3. Következtetések

Kutatásom egyik központi célkitűzése az 5. kutatási kérdés vizsgálata volt, miszerint az internetkapcsolattal rendelkező járművek kommunikációs protokolljai – azok alacsony késleltetésű és erőforrás-hatékony működése miatt – potenciálisan lehetőséget biztosítanak rejtett kommunikációs csatornák létrehozására. Ennek vizsgálatához három eltérő adattípust (vizuális – képek, hangalapú – audiofelvételek, valamint helymeghatározási – GPS-adatok) elemeztem, az MQTT protokoll kontextusában. Feltételezésem szerint a vizsgált jármű szoftverarchitektúrájának valamely kritikus eleme kompromittálódott, így a támadó teljes hozzáféréssel rendelkezik a telematikai alrendszer adatfolyamaihoz, és képes azokat manipulálni.

A modellalkotás során a rejtett csatornák sávszélességének becslésére helyeztem a hangsúlyt, figyelembe véve az adattípusok eltérő terjedelmét és a szoftveres működés realitásait. Bár az 5G-kommunikáció lehetővé tenné akár nagy volumenű adatok átvitelét is, a modell konzervatív keretek között marad: az adatátviteli lehetőségek vizsgálatánál kizárólag a protokoll technológiai adottságaira és az adatok struktúrájára összpontosítottam, a hálózati infrastruktúra korlátozása nélkül.

Az eredmények rávilágítottak, hogy míg képek és hangfelvételek rejtett továbbítása jelenleg jelentős sávszélességi igénnyel jár, így csak ritkán és hosszabb időkeretekben lenne kivitelezhető, addig a geolokációs adatok – strukturált jellegük és kis méretük miatt – kiválóan alkalmasak rejtett csatornás továbbításra. Ezek különösen nehezen detektálhatók, mivel a jármű működésének részét képező szenzoralapú adatforgalommal vizuálisan és statisztikailag is jól álcázhatók. Ezzel közvetlenül alátámasztásra kerül a T4 tézis azon állítása, hogy a titkosítás önmagában nem elegendő a rejtett kommunikáció kizárására, ezért célzott védelmi mechanizmusok – például anomáliaalapú forgalomelemzés – bevezetése elengedhetetlen.

A modellezés igazolja, hogy az internetkapcsolatra képes járművek fejlett szoftverarchitektúrája és kommunikációs protokolljai – különösen flottaszintű működés esetén – rejtett csatornák kihasználásával jelentős mennyiségű, érzékeny adat észrevétlen továbbítására képesek. Az egyes adattípusok, mint például a geolokációs adatok, különösen alkalmasak erre, mivel strukturált és kisméretű voltuk miatt hatékonyan álcázhatók a rendszeres adatforgalomban.

Mindezek alapján a kutatási kérdésből az alábbi tézis (T5) fogalmazható meg: A dolgozatban bemutatott modell alapján megállapítható, hogy az internetre kapcsolt személygépjárművek – különösen a fejlett vezetéstámogató rendszerekkel rendelkező járművek – képesek rejtett módon nagy mennyiségű érzékeny adat továbbítására, amely flottaszinten kritikus nemzetbiztonsági kockázatot jelenthet kijelölt objektumok vagy célszemélyek megfigyelése esetén. Ez a felismerés rávilágít arra, hogy a jelenlegi védelmi mechanizmusok kiegészítése, valamint célzott, anomáliadetektáló eszközök fejlesztése elengedhetetlen a jövőbeni adatbiztonság garantálásához.

7. MEGOLDÁSI JAVASLAT: HATÓSÁGI FELÜGYELETTEL ÖSSZEKÖTÖTT ÁTFOGÓ KOCKÁZATELEMZÉS

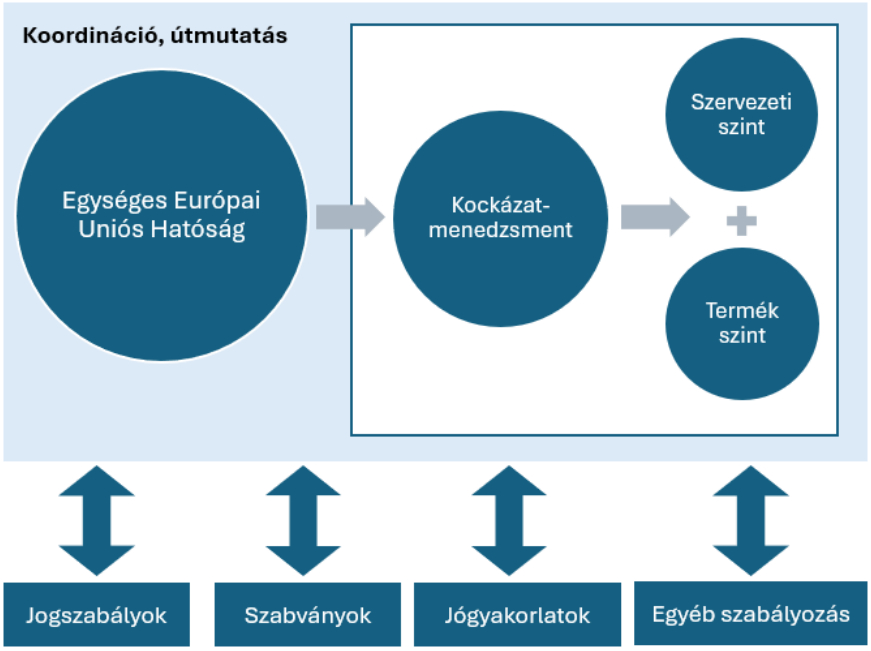
A kockázatelemzési és hatósági kihívások integrált értelmezésével foglalkozó kutatási szakasz célja annak vizsgálata volt, hogy Milyen korlátai vannak a jelenleg alkalmazott járműipari kockázatelemzési módszereknek az internetkapcsolattal rendelkező járművek komplex információbiztonsági kockázatainak kezelésében? A kutatási kérdésre adott válaszkeresés megalapozta az elemzési irányokat, és hozzájárult a vizsgálat struktúrájának kialakításához.

Az okosjárművek elterjedésével jelentős mértékben megnőtt az általuk gyűjtött és kezelt adatok mennyisége, amelyek nagy része üzleti szempontból vagy személyes adatvédelmi szempontból érzékeny. Ezen adatok kezeléséhez olyan fejlett kockázatelemzési módszertanok alkalmazása szükséges, amelyek lehetővé teszik az adatvédelmi aggályok hatékony kezelését, különösen azokban az adatgyűjtési és -kezelési pontokban, amelyek magas adatvédelmi vagy információbiztonsági kockázattal járnak.

A dolgozat során alkalmazott kvalitatív (mélyinterjús) és kvantitatív (kérdőíves, modellalapú) kutatási módszerek egyaránt azt igazolták, hogy az internetkapcsolattal rendelkező személygépjárművek információbiztonsági kockázatai komplex, többdimenziós problémaként értelmezhetők. A szakértői vélemények alapján egyértelművé vált, hogy a jelenlegi szabványok és gyakorlatok nem biztosítanak elegendő védelmet a járművekben keletkező vagy onnan továbbított érzékeny adatokkal szemben – különösen, ha rejtett adatcsatornák kihasználásáról van szó. A kidolgozott modell pedig arra mutatott rá, hogy ezek az adatok – megfelelő sávszélességgel – nem csupán elméletileg, hanem gyakorlati szinten is visszaélésre alkalmas mennyiségben továbbíthatók. Mindebből világosan következik, hogy az ilyen típusú fenyegetések nem kezelhetők kizárólag technikai védelmi eszközökkel, és nem háríthatók pusztán a felhasználók tájékozottságára vagy felelősségére. A járműipari kiberbiztonság megerősítéséhez elengedhetetlen egy integrált, hatósági felügyelettel összekötött, ciklikusan alkalmazott kockázatértékelési és -kezelési módszertan, amely az adatok teljes életciklusát figyelembe véve biztosítja a személyes és üzleti adatok védelmét, valamint az ágazati bizalom fenntarthatóságát.

A fentiek alapján egyértelművé vált, hogy az internetkapcsolatra képes járműipar kiberbiztonsági kihívásaira adott válaszok sem intézményi, sem módszertani szinten nem

lehetnek egymástól függetlenek. A kutatási kérdések vizsgálata során minden elemzés oda vezetett, hogy a teljeskörű biztonsági megfelelés, legyen szó társadalmi, jogi, technikai vagy műszaki aspektusról, csakis akkor valósítható meg, ha egyrészt létrejön egy világos hatósági-intézményi keret, amely egyértelműen meghatározza a szereplők feladatait, felelősségeit, jogosítványait, és biztosítja a koordinációt és transzparenciát; másrészt kialakításra kerül egy olyan integrált kockázatmenedzsment-keretrendszer, amely képes összekapcsolni a szervezeti és termékszintű kockázatértékelést, egységesíteni az auditálási folyamatokat, és valós visszacsatolást adni a szabályozási és gyakorlati problémákra (11. ábra).



11. ábra - Javasolt struktúra: Egységes hatóság és integrált kockázatmenedzsment rendszer. Forrás: saját forrás.

A dolgozatban bemutatott kutatás igazolja, hogy csak e két alappillér – a hatóság megfelelő működése és a korszerű, integrált kockázatmenedzsment – együttes megléte képes az ágazat valamennyi kihívását lefedni. E kettős megközelítésnek kell a jövőbeni szabályozási és megfelelési gyakorlat középpontjában állnia, s minden egyes megfelelési követelménynek, szabványnak, illetve audit- vagy tanúsítási folyamatnak ezekhez a fundamentumokhoz kell igazodnia.

7.1. Hatósági felügyelet és támogatás

Az internetkapcsolatra képes személygépjárművek kiberbiztonsági szabályozása globális szinten is összetett kihívás, mivel a nemzeti jogrendszerek, beszállítói láncok és technológiai megoldások sokszínűsége gyakran átfedéseket és ellentmondásokat

eredményez. Az Európai Unióban ez különösen szembetűnő a harmadik országokból – főként Kínából – érkező technológiák térnyerése miatt, amelyek új, sokszor kezeletlen kockázatokat hoznak felszínre. Kínában a Cybersecurity Law, a Data Security Law és a Personal Information Protection Law (PIPL) [232]–[235] egy centralizált, államilag irányított rendszer alapját képezik. A központi szabályozás gyors reagálást tesz lehetővé, de a transzparencia és a független audit hiánya, valamint a nemzetbiztonsági prioritások dominanciája korlátozza a fogyasztói és beszállítói jogok érvényesülését [233], [236]. Az európai típusú elvek, mint a *privacy by design* vagy az adatminimalizálás, csak korlátozottan jelennek meg [232], [233]. Az Egyesült Államokban a szabályozás decentralizált és önszabályozásra épülő. Az NHTSA és a NIST iránymutatásai [237], [238] adják a keretet, az innovációs rugalmasság viszont a supply chain kiberbiztonság és a tanúsítási folyamatok széttagoltságával jár. A felelősségi körök sokszor nem tisztázottak, ami rendszerszintű sérülékenységeket okozhat [237]. Japánban a szabályozás technológiaorientált, és az iparági együttműködésen (pl. JASPAR, JAMA) alapul [239]. A hosszú távú OEM–beszállító partnerségek és a minőségbiztosítás erősek, de a nemzetközi harmonizáció és a független auditmechanizmusok kevésbé hangsúlyosak. Az Európai Unióban a jogi háttér – GDPR, UNECE R155/R156, NIS2, CRA – elviekben magas szintű, de a gyakorlatban széttöredezett. A tagállamok között jelentős eltérések vannak a kockázatelemzés, auditálás és tanúsítás terén, különösen a beszállítói lánc biztonságát és az EU-n kívüli gyártók ellenőrzését illetően [240]–[243]. A szakirodalom [241], [243] szerint ez a széttagoltság hátráltatja az egységes kockázatmenedzsmentet, és fokozza a felelősségi bizonytalanságokat.

Egyre több tanulmány sürget központi, koordinált hatósági és módszertani megközelítést, amely egységesítené a szabályozási eljárásokat, auditálási gyakorlatokat és kockázatkezelést [242]–[246]. Az integrált, életciklus-alapú modell iránti igény erősödik, amely támogatná a valós idejű, határokon átnyúló kiberbiztonsági megfelelést az okosjármű-ökoszisztémában.

Jelenleg az EU-ban a járműipari felügyelet többszintű és tagállami szinten eltérő. A szabályozást nem központi hatóság, hanem nemzeti szervezetek végzik, amelyek eltérő hatáskörrel rendelkeznek [247], [248]. A típusjóváhagyási szervezetek főként technikai megfelelést ellenőriznek, a kiberbiztonsági szempontokat (UNECE R155/R156) viszont csak részben integrálták [249].

Az iparági hálózatok és tanácsok – például a beszállítói lánc biztonsági fóruma – inkább önszabályozó tudásmegosztó szervezetek, hatósági jogosítvány nélkül [250]. A NIS2 irányelv keretében kijelölt nemzeti hatóságok (pl. CERT-ek, minisztériumok) nem rendelkeznek kifejezetten autóipari kompetenciával [250], [251]. Az adatvédelmi hatóságok (DPAs) függetlenül működnek, a járműipari szabályozással való együttműködésük többnyire eseti jellegű [252]. Az ENISA iránymutatásokat ad, de nem rendelkezik ellenőrzési jogkörrel [250].

A CRA végrehajtását tagállami piacfelügyeleti hatóságok és új európai megfelelőségi szervezetek fogják ellátni, de pontos feladatkörük és együttműködési mechanizmusuk még kialakítás alatt áll [253].

Mindezek alapján egy korszerű, átfogó kiberbiztonsági hatósági modellnek több együttműködési szinten kell működnie. A különböző szinteket a 10. táblázatban szemléltetem. Egyrészt stratégiai szinten formalizált kapcsolatot kell kialakítania a nemzeti és európai hatóságokkal (NIS2-hatóságok, DPAs, ENISA, CRA-szervek), egységes audit- és tanúsítási módszertanokkal, közös eljárásrendekkel és hatáskör-megosztással [250], [251]. Másodsorban szakmai, hálózati szinten együtt kell működnie az iparági tanácsokkal, OEM-ekkel, beszállítókkal, szervizhálózatokkal, kamarákkal. A modell alapelve, hogy a felelősségi viszonyokat és a tudásmegosztást minden rétegben folyamatosan aktualizálni kell, támogatva a dinamikus ökoszisztéma működését [249]. Harmadrészt operatív szinten fontos az auditálási, megfelelőségi és gyors reagálási folyamatok támogatása, végül – bár kevésbé hangsúlyosan – a társadalmi edukációban, biztonságtudatosság-növelésben is szerepet kell vállalni [250], [252].

Együttműködési szint	Kapcsolódó szervezetek / szereplők	Főbb feladatok, példák
Stratégiai, szabályozói	NIS2 nemzeti hatóságok, ENISA, DPAs, CRA hatóságok, európai típusjóváhagyási szervek	Jogértelmezési együttműködés; közös audit- és tanúsítási módszertan kialakítása; szankcionálási mechanizmusok kialakítása; technikai ajánlások, irányelvek kidolgozása; szabályozási átfedések kezelése; nemzeti hatóságok koordinálása, jelentések fogadása
Iparági, szakmai	ISAAC-ek, OEM-ek (gyártók), beszállítók, szakmai kamarák, szervizek, kereskedői hálózatok, autószerelői szakszervezetek	Jógyakorlatok és követelményrendszerek kidolgozása; szakmai képzés, tudásmegosztás; technikai útmutatók kiadása; piaci szereplők támogatása a megfelelőség elérésében; szakmai hálózatépítés; felelősségi viszonyok egyeztetése

Együttműködési szint	Kapcsolódó szervezetek / szereplők	Főbb feladatok, példák
Operatív, gyakorlati	OEM-ek (járműgyártók), elsődleges és másodlagos beszállítók, szervizpartnerek	Auditálás egységes módszertan szerint; auditfolyamatok és megfelelőségi projektek támogatása; gyors reagálási folyamatok (rapid response); visszacsatolás a szereplőktől; technikai ajánlások bevezetése
Publikus, edukációs	Lakosság, végfelhasználók, civil szervezetek, oktatási intézmények	Edukációs programok, szakmai és lakossági rendezvények; tudatosság-növelés, ismeretterjesztés

10. táblázat - Hatósági feladatok leírása együttműködési szintenként. Forrás: saját forrás.

A szakirodalom egyértelműen rámutat, hogy az ágazati kiberbiztonság csak akkor hatékony, ha a szabályozás, a szakmai gyakorlat és az auditálás között folyamatos, kétirányú visszacsatolás és tudásmegosztás működik [254], [255]. A járműipari kiberbiztonság összetettsége abból fakad, hogy a szabályozási, technikai és szervezeti szintek töredezettek, ezért számos kritikus probléma nem kezelhető egységes módszertannal. Az egyik legfőbb akadály a párhuzamos, koordinálatlan előírások és hatósági követelmények rendszere, amely átláthatatlanságot és információs aszimmetriát eredményez mind a piaci szereplők, mind a végfelhasználók számára.

Az empirikus vizsgálatok és interjúk szerint az egységes kockázatelemzési módszertan hiánya a legjelentősebb probléma: a legtöbb OEM és beszállító ad-hoc, nem harmonizált eljárásokat alkalmaz, így a tényleges fenyegetések gyakran rejtve maradnak. Műszaki szinten jellemző, hogy egyes kommunikációs protokollokból hiányzik a titkosítás, vagy nem felelnek meg a korszerű támadási mintáknak. A dolgozat modellezési eredményei azt is mutatják, hogy még a korszerű titkosítás és hozzáférés-szabályozás sem nyújt védelmet minden fenyegetéssel szemben – például ha állami vagy privilegizált szereplők rejtett csatornákat (*covert channel*) használnak az adatküldési infrastruktúrában. Ezért a kockázatelemzésnek rendszerszinten és nem konvencionális vektorokra is kiterjedően kell működnie.

A 10. Mellékletben összefoglaltam azokat a gyakorlati megoldási javaslatokat, amelyek iránymutatásként szolgálhatnak egy jövőbeli rendszer kialakításához.

7.2. Integrált kockázatmenedzsment modell

Az internetkapcsolatra képes járműipar kiberbiztonsági megfelelőségének egyik legkritikusabb pontja a kockázatelemzés módszertani színvonala és tényleges gyakorlati alkalmazhatósága. A dolgozat empirikus kutatásai, valamint az iparági interjúk tapasztalatai azt mutatják, hogy jelenleg a kockázatelemzés két, részben elszigetelt szinten zajlik: egyrészt a szervezeti szintű folyamatokat és struktúrákat vizsgálják, másrészt a konkrét termékekhez – jellemzően a TARA (Threat Analysis and Risk Assessment) módszertan szerint – kapcsolódó fenyegetéseket elemzik. Ez a szétválasztás azonban oda vezet, hogy a szervezeti működésből eredő, összetettebb, rendszerszintű kockázatok és a konkrét termékmegvalósítások közötti kapcsolatok sok esetben rejtve maradnak, az elemzésekben pedig gyakran előfordul, hogy a valós fenyegetések helyett kizárólag általános, tankönyvi példák kerülnek beazonosításra. A doktori kutatás egyik legfontosabb tudományos és gyakorlati újítása ezért egy olyan integrált kockázatmenedzsment-keretrendszer kialakítása, amely lehetővé teszi a szervezeti és termékszintű elemzések egységesítését, a folyamatok és termékek közötti visszacsatolást, valamint egy olyan auditmódszertan kidolgozását, amely a kockázatelemzés valódi mélységét, relevanciáját és gyakorlati alkalmazhatóságát garantálja. Az így létrejövő rendszer nemcsak a megfelelőség formális biztosítását teszi lehetővé, hanem ténylegesen hozzájárul a járműipar kiberrezilienciájának növeléséhez is.

A dolgozatban javasolt integrált kockázatmenedzsment-keretrendszer tudományos újdonsága abban ragadható meg, hogy képes összehangolni a szervezeti és termékszintű kockázatelemzési gyakorlatokat, mindezt egy adaptív és iteratív modellben, amely folyamatos visszacsatolást és naprakészségét biztosítja. Az elméleti modell egyik alapvetése, hogy a járműiparban alkalmazott kockázatelemzés nem tekinthető statikus, egy ponton lezárt folyamatnak, hanem a fenyegetési környezet változásait, a technológiai fejlődést és a piaci szereplők visszajelzéseit is figyelembe vevő, dinamikus rendszerként kell működnie. Ezt támasztják alá Wang és munkatársai is, akik egy olyan átfogó kockázatfelmérési keretrendszert mutatnak be, amely a járművek teljes életciklusán keresztül képes azonosítani és rangsorolni a különböző fenyegetéseket, kvantitatív és kvalitatív módszerek integrálásával [254]. A kutatási eredmények rámutatnak arra is, hogy az auditálási és megfelelőségi folyamatokat csak abban az esetben lehet valóban hatékonnyá tenni, ha a biztonsági követelmények menedzsmentje formalizált,

automatizált és transzparens, ahogy azt Luo és szerzőtársai is kiemelik: egy olyan követelménykezelési rendszer, amely automatizáltan képes fenyegetéseket észlelni, és ezek alapján naprakész megfelelőségi értékelést készíteni, jelentős mértékben csökkenti a kockázatok „elfedésének” esélyét és a megfelelési folyamatok formálissá válását [255]. Ezzel párhuzamosan Shiwakoti és munkatársai rendszerszintű modellezésen alapuló keretrendszert dolgoztak ki, amely lehetővé teszi, hogy a szervezetek a technológiai, emberi és irányítási tényezők együttes figyelembevételével iteratív módon reagáljanak a kiberbiztonsági kihívásokra; a szerzők szerint e megközelítés a folyamatos monitoringot, auditot és gyors reagálást is támogatja, meghaladva a pusztán reaktív, ex-ante megfelelőségi paradigmát [256]. A fenti elméleti keret újdonsága tehát abban áll, hogy a szervezeti, technológiai és emberi tényezők integrált értelmezése révén adaptív és fenntartható kockázatkezelést tesz lehetővé, amelyben a hatóság és a piaci szereplők közötti kétirányú visszacsatolás folyamatos tudásmegosztást, szabályozási és módszertani fejlesztést eredményez.

Az integrált kockázatmenedzsment rendszer bevezetése jelentős előrelépést jelent a járműipari kiberbiztonság területén, de számos, a jövőben kutatandó módszertani és technológiai kérdést vet fel. Az egyik legfontosabb kutatási irány a valós idejű adatáramlások gépi tanulás-alapú monitorozása, amely lehetővé teszi a járművek belső hálózataiban (IVN) zajló események folyamatos felügyeletét, és automatikusan képes felismerni a szokatlan vagy gyanús viselkedési mintákat. Alfardus és Rawat (2024) eredményei szerint a deep learning-alapú anomáliadetektálás hatékonyan képes valós időben kiszűrni a járműhálózati támadásokat, ezzel jelentősen növelve a rendszer rezilienciáját [257].

A második kulcsfontosságú kutatási terület az automatizált auditálási és gyors reagálási képességek fejlesztése. Az ilyen rendszerek a diagnosztikai adatok manipulációját képesek valós időben felismerni, ahogyan azt egy intelligens, többlépcsős keretrendszerrel mutatja be egy friss, GAN és XGBoost alapú, járműdiagnosztikára specializált tanulmány [258]. Ez a megközelítés ideális példája a kockázatelemzési, auditálási és válaszadási folyamatok automatizálásának, amely nélkülözhetetlen lesz a jövőben az egyre komplexebb támadási formákkal szemben.

Szintén kiemelendő irány a kockázati szintek automatizált besorolása: Aloqaily és munkatársai (2025) különböző felügyelt gépi tanulási algoritmusokat alkalmaznak a

járművek hálózati forgalmának valós idejű támadásdetektálására, amely nemcsak az azonnali felismerést, hanem a gyors kockázati besorolást is lehetővé teszi [259]. Ezek az újgenerációs, automatizált megoldások az integrált kockázatmenedzsment rendszer szerves részét képezhetik a következő években. Metaszinten a dolgozatban bemutatott modell adaptálhatósága különös jelentőséggel bír más, kritikus infrastruktúrák és IoT ökoszisztémák számára is. Az egészségügyi IoT, az ipari irányítástechnika vagy az okosváros-projektek területén is hasonlóan jelennek meg a szervezeti és technológiai szintek közötti átjárhatóság, a formális megfelelőség és az átlátható, automatizált kockázatmenedzsment iránti igények. A valós idejű adatmonitorozás, az automatizált auditálás és a dinamikusan fejlődő tudásbázisok kialakítása ezekben a szektorokban is nélkülözhetetlen lesz a fenyegetési környezet hatékony kezeléséhez és az ökoszisztéma szintű biztonság növeléséhez.

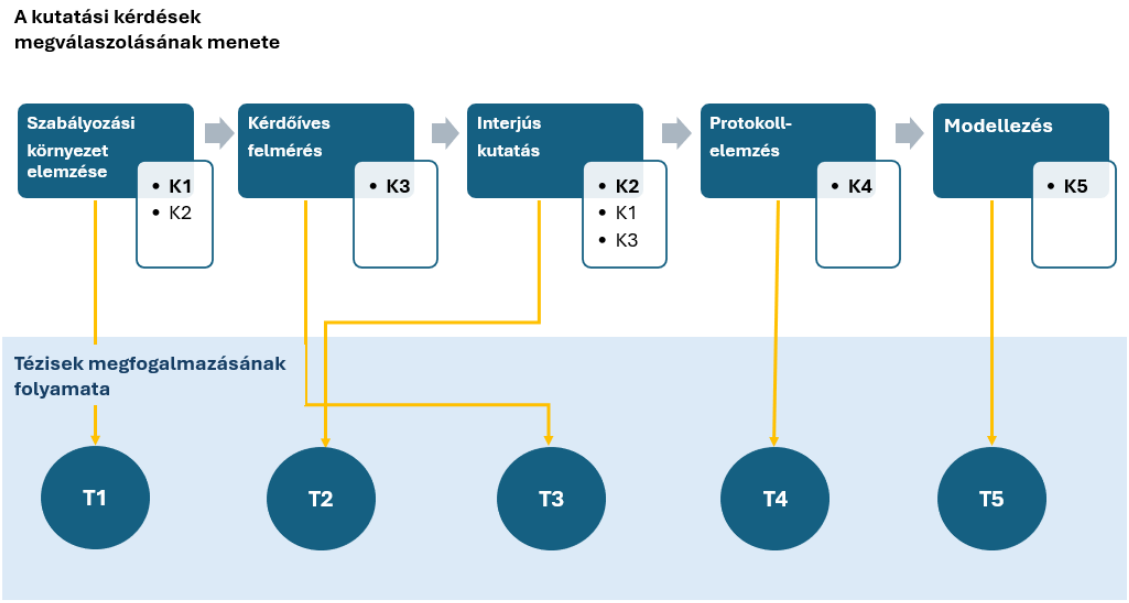
8. ÚJ TUDOMÁNYOS EREDMÉNYEK, TÉZISEK

A kutatás célja az volt, hogy feltárjam az internetkapcsolattal rendelkező személygépjárművek információbiztonsági kockázatait, és megvizsgáljam, miként reagál erre a szabályozási, technológiai és felhasználói környezet.

A célok eléréséhez több, egymást kiegészítő módszertant alkalmaztam, amelyek lehetővé tették a probléma több szintű elemzését. A kutatási kérdések és tézisek kapcsolatát a 12. ábra szemlélteti, amely bemutatja, miként vezetett a különböző módszertani lépések sora a tézisek megfogalmazásához.

Bár a kutatási terv lineáris logikát követett, a gyakorlatban a folyamat iteratív, egymásra épülő és reflexív módon valósult meg. A szabályozási környezet elemzése (K1) a tartalomelemzés módszertanával megalapozta a T1 tézist, míg a K2 kérdéshez szakértői interjúk bevonása is szükséges volt.

A kérdőíves felmérés (K3) a felhasználói tudatosság és attitűdök vizsgálatára szolgált, az interjús kutatás pedig megerősítette a K1–K3 kérdésekhez kapcsolódó eredményeket. A protokollelemzés (K4) és a modellezés (K5) módszerei közvetlenül támogatták a T4 és T5 tézisek kidolgozását, igazolva a kutatási terv komplexitását.



12. ábra - A kutatási kérdések megválaszolásának menete és a tézisek felállításának folyamata. Forrás: saját forrás.

A K1–K2 kérdések vizsgálata során tematikus tartalomelemzéssel elemeztem a főbb szabályozásokat és szabványokat (pl. ISO/SAE 21434, UNECE R155/R156, GDPR, TISAX, Cyber Resilience Act), értékelve azok alkalmasságát az új típusú kockázatok kezelésére. A K3 kérdőíves kutatás a járműhasználók adatbiztonsági tudatosságát és viszonyulását vizsgálta, míg a K2–K3 interjúk a gyakorlati tapasztalatokat és a megfelelés nehézségeit tárták fel. A K4 protokollelemzés során a járműkommunikációs architektúrákat vizsgáltam a rejtett adatátvitel (covert channels) lehetőségei szempontjából.

Végül a K5 kérdéshez egy Poisson-folyamaton és random waypoint elméleten alapuló modell segítségével szimuláltam az adatátvitel mintázatait, különös tekintettel a flottaszintű kockázatokra.

A kutatás több módszert kombinált annak érdekében, hogy a járművek információbiztonsági kihívásait rendszerszinten lehessen értelmezni. A kvalitatív és kvantitatív eredmények egymást erősítve alapozták meg az alábbi téziseket:

T1: Az Európai Unió jelenleg érvényes szabályozási környezete hézagos, csak foltszerű védelmet képes nyújtani a személygépjárművekkel kapcsolatos ismert fenyegetések ellen.

[HH1], [HH2], [HH3]

T2: A szabályozások által elvárt kockázatelemzési módszerek nem alkalmasak az internetkapcsolatra képes személygépjárművekkel kapcsolatos összes kockázat kezelésére, mivel vagy csak a járműre, vagy csak a szervezetre fókuszálnak és használatukat nem ellenőrzi egységes hatóság.

[HH1], [HH2], [HH3]

T3: Az internetkapcsolatra képes járművek vásárlói nem kapnak megfelelő tájékoztatást a biztonsági kockázatokkal kapcsolatban, elsősorban a technológia fejlődésből adódó kényelmi funkciókra koncentrálnak, így nem fordítanak figyelmet a kockázatokra.

[HH4], [HH5], [HH6]

T4: Az internetkapcsolattal rendelkező járművek kommunikációs protokolljai – funkcionális követelményeik (pl. alacsony késleltetés, korlátozott erőforrás-használat) miatt – alkalmasak rejtett csatornák létrehozására, amelyek technikai védelmi eszközökkel, például titkosítással, nem szüntethetők meg teljes mértékben. Ezért a rejtett csatornák azonosítása és célzott védelmi intézkedések kidolgozása elengedhetetlen a járműkommunikáció biztonságának fenntartásához.

[HH7], [HH8]

T5: A dolgozatban bemutatott modell alapján megállapítható, hogy az internetre kapcsolt személygépjárművek – különösen a fejlett vezetéstámogató rendszerekkel rendelkező járművek – képesek rejtett módon nagy mennyiségű érzékeny adat továbbítására, amely flottaszinten kritikus nemzetbiztonsági kockázatot jelenthet kijelölt objektumok vagy célszemélyek megfigyelése esetén.

[HH9]

A kutatás eredményei több jövőbeli irányt jelölnek ki. A T4–T5 tézisek alapján indokolt a rejtett adatátvitelt automatikusan detektáló megoldások (pl. gépi tanulás, viselkedéselemzés) fejlesztése, valamint a különböző járműarchitektúrák összehasonlító biztonsági elemzése. Fontos lenne olyan szteganográfiai felismerő mechanizmusok integrálása is, amelyek közvetlenül a kommunikációs protokollokba építhetők.

A felhasználói edukáció hiányai új kutatási irányokat nyithatnak – például dinamikus hozzáférés-kezelési és adaptív adatvédelmi modellek kidolgozását. Emellett a flottaszintű

megfigyelés és a kritikus infrastruktúrák elleni kockázatok vizsgálata is további kutatási potenciált kínál.

A szabályozási hiányosságok alapján javasolt egy integrált, több szintű kockázatelemzési keretrendszer kidolgozása, amely egyesíti a jármű-, szervezeti-, ökoszisztéma- és hatósági kontrollokat. Ennek vizsgálata kiterjedhet a pilot jellegű auditálási modellekre és a központosított hatósági ellenőrzések hatékonyságára is. A cél egy átlátható, auditálható, valós körülmények között is működő felügyeleti rendszer kialakítása, amely biztosítja az egységes és számonkérhető megfelelést az EU-ban és a harmadik országok járművei esetében is.

9. SAJÁT PUBLIKÁCIÓK

[HH1] H. Hegyi, "Elektromos járművek töltőinfrastruktúrája: Kiberbiztonsági fenyegetések és geopolitikai összefüggések," in VI. Eurázsia hajnala konferencia Absztraktfüzet, Budapest, Neumann János Egyetem, Eurázsia Központ, 2024, pp. 20–21.

[HH2] H. Hegyi, "A Kelet és a Kód: Kína elektromos autóinak európai terjeszkedése az informatikai biztonság tekintetében," in Absztraktfüzet - Eurázsia Hajnala, Budapest, Neumann János Egyetem, Eurázsia Központ, 2023, p. 16.

[HH3] H. Hegyi, "A kínai elektromos személygépjárművek elterjedésének információbiztonsági kihívásai az Európai Unióban," Eurázsia Szemle, vol. 3, no. 3, pp. 30–50, 2023.

[HH4] H. Hegyi, "A személygépjárművek információbiztonsága az információbiztonsági szakértők szemszögéből," Biztonságtudományi Szemle, vol. 5, no. 2, pp. 47–58, 2023.

[HH5] H. Hegyi, L. Erdődi, "Connected and Exposed: Cybersecurity Risks, Regulatory Gaps, and Public Perception in Internet-Connected Vehicles," arXiv preprint arXiv:submit/6685891 [cs.CR], Aug. 2025.

[HH6] H. Hegyi, "A Qualitative Study Investigating Data Security Measures in the European Union," Academic and Applied Research in Military and Public Management Science, vol. 23, no. 2, pp. 63–75, 2024.

[HH7] H. Hegyi and L. Erdődi, "Személygépjárművek adatforgalmának megfigyelési célú felhasználási lehetőségei," Biztonságtudományi Szemle, vol. 5, no. 1, pp. 53–67, 2023.

[HH8] H. Hegyi, "Modernizáció és iparbiztonság a COVID-19-járvány után Magyarországon," in Digitális Biztonságpolitika a Kibertérben, T. Babos, Ed. Gödöllő: Magyar Agrár- és Élettudományi Egyetem, 2021, pp. 101–131.

[HH9] H. Hegyi and L. Erdődi, "Modern Passenger Vehicles as Cyber Threat Source: Analyses of Surveillance Options through Smart Vehicles," Acta Polytechnica Hungarica, vol. 22, no. 2, pp. 9–28, 2025.

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

[5] 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.

[6] Bódi, A., Maros, D., & Gáspár, L. (2023). A közlekedésbiztonság fokozása a Komplex ITS Ökoszisztémával. KTI Magyar Közlekedéstudományi és Logisztikai Intézet.

[7] Bódi, A. (2022). Közlekedésbiztonság fokozását megalapozó Komplex ITS Ökoszisztéma kialakításának kérdései. Doktori értekezés, Óbudai Egyetem, Biztonságtudományi Doktori Iskola.

[8]Bloom, C., Tan, J., Ramjohn, J., & Bauer, L. (2017). Self-driving cars and data collection: Privacy perceptions of networked autonomous vehicles. USENIX Symposium on Usable Privacy and Security.

[9] Bódi, A., & Maros, D. (2022). A közös európai mobilitási adattér és az ITS ökoszisztéma tanúsíthatósága. Közlekedés és Mobilitás, 1(1), 38–42.

[10] Krasznay, Cs. (2022). Kiberbiztonság a XXI. században. Katonai Nemzetbiztonsági Szolgálat.

[11] Krasznay, Cs. (2020). Okoseszközök a kritikus információs infrastruktúrákban. In Török, B. (szerk.), Információ- és kiberbiztonság (pp. 121–147). Ludovika Egyetemi Kiadó.

[12] Kovács, L., & Krasznay, Cs. (2010). Digitális Mohács – Egy kibertámadási forgatókönyv Magyarország ellen. Nemzet és Biztonság, 2010. február.

[13] Bódi, A., & Maros, D. (2021). Az 5G-hálózat és a közlekedés információbiztonsági kihívásai. Híradástechnika, 76(HTE Infokom 2020), 35–40.

[14] Török, Á., Szalay, Z., & Sághi, B. (2020). New Aspects of Integrity Levels in Automotive Industry-Cybersecurity of Automated Vehicles. IEEE Transactions on Intelligent Transportation Systems.

[15] Jekl, B., Dabčević, Z., Németh, B., Škugor, B., & Gáspár, P. (2025). Scenario-Optimization-Based Velocity Planning of Autonomous Vehicles for Interacting With Pedestrians. IEEE Transactions on Intelligent Transportation Systems.

[16]Caltrider, J.; Rykov, M.; MacDonald, Z.: What Data Does My Car Collect About Me and Where Does It Go? Mozilla Foundation, 2023.

[17]Bódi, A., & Bartal, A. (2022). Az okosjárművek adatkezelésének kérdései. Információs Társadalom, 22(1), 21-40.

[18] A. Stocker, C. Kaiser, M. Fellmann, “Quantified Vehicles: Novel Services for Vehicle Lifecycle Data,” Business & Information Systems Engineering, vol. 59, pp. 125–130, 2017. https://www.researchgate.net/publication/313546098_Quantified_Vehicles_Novel_Services_for_Vehicle_Lifecycle_Data

[19] B. Gözübüyük, B. Tang, K. G. Shin, M. D. Pesé, “Analyzing Privacy Implications of Data Collection in Android Automotive OS,” 2024. https://arxiv.org/abs/2409.15561

[20] T. Alam, “Data Privacy and Security in Autonomous Connected Vehicles,” Data Journals, vol. 8, no. 9, 2024. https://www.mdpi.com/2504-2289/8/9/95

[21] N. Yuca et al., “A Survey on Privacy-Preserving Computing in the Automotive Domain,” 2025. https://arxiv.org/abs/2508.01798

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

[23] Wired: GM Took 5 Years to Fix a Full-Takeover Hack on Millions of OnStar Cars. URL: 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.)

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

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

[26] Mercator Institute for China Studies, „Europe's position in global EV market”, 2021.

[27]H. Hegyi, „Cybersecurity Challenges in the Era of Chinese Electric Passenger Vehicles: A Qualitative Study Investigating Data Security Measures in the European Union,” AARMS, vol. 23, no. 2, pp. 63–75, 2024, doi: 10.32565/aarms.2024.2.5.

[28] S&P Global Mobility, “The rise of Chinese auto brands in Europe,” 2023.

[29] European Automobile Manufacturers Association (ACEA), “Market Report 2024,”

[30] JATO Dynamics, “Chinese automakers double European market share in May,” 2025.

[31] Fleetnews, “Chinese brands gain ground and double market share across Europe,” May 2025.

[32] JATO Dynamics, “European registrations of Chinese car brands soar in January,” Jan. 2025.

[33] Reuters, “China's carmakers expanding their presence in Europe,” July 2025.

[34] The Times, “BYD electric cars overtake Tesla sales in Europe,” Apr. 2025.
[chinacarOnline

[35] Reuters, “Tesla's European sales slump for fifth month,” June 2025.

[36] European Commission, “Countervailing duties on Chinese EV imports,” 2024.

[37] Wikipedia contributors, “Automotive industry in China,” Wikipedia, 2025.

[38] Államtanács, „Stratégiai feltörekvő iparágak fejlesztése Kínában”, 2010.

[39] S. Curry, „Web application vulnerabilities in vehicles”, 2023.

[40] European Commission, „EU-China – A strategic outlook”, 2022.

[41] J. Mock, Z. Yang, „China's electric vehicle market policies”, Energy Policy, 2021.

[42] ACEA, „EU car imports overview”, 2021.

[43] ENISA, „Cybersecurity Certification and ENISA’s Role”, 2022.

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

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

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

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

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

[49] 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.

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

[51] 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.

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

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

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

[55] G. Danezis, Introduction to Privacy Technology. KU Leuven COSIC Lecture, 2007. [1SPOnline

[56] M. Deng, K. Wuyts, R. Scandariato, B. Preneel, W. Joosen, “A privacy threat analysis framework: supporting the elicitation and fulfillment of privacy requirements,” Requirements Engineering, vol. 16, no. 1, pp. 3–32, 2011.

[57] C. Lázaro, D. Le Métayer, “Control over Personal Data: True Remedy or Fairy Tale?” SCRIPTed, vol. 12, no. 1, pp. 3–30, 2015.

[58] M. Raciti and G. Bella, “Up-to-date Threat Modelling for Soft Privacy on Smart Cars,” arXiv, 2023. [SPOnline

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

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

[61] K. W. Abbott and D. Snidal, “Hard and Soft Law in International Governance,” International Organization, vol. 54, no. 3, pp. 421–456, 2000.

[62] A. Peters and R. Pagotto, “Soft Law as a New Mode of Governance,” New Modes of Governance Project, 2006.

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

[64] U. Kischel, Comparative Law. Oxford, U.K.: Oxford Univ. Press, 2019.

[65] C.-L. Hwang and K. Yoon, Multiple Attribute Decision Making: Methods and Applications. Berlin, Germany: Springer, 1981.

[66] ENISA, Threat Landscape for Connected and Automated Mobility. Athens, Greece: European Union Agency for Cybersecurity, 2021.

[67] OECD, Regulatory Impact Analysis (RIA): Best Practice Principles for Regulatory Policy. Paris, France: OECD Publishing, 2020.

[68] V. Belton and T. J. Stewart, Multiple Criteria Decision Analysis: An Integrated Approach. Boston, MA, USA: Springer, 2002.

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

[70]Lincoln, Y. S., & Guba, E. G. (1985). Naturalistic Inquiry. Sage.

[71]Patton, M. Q. (2015). Qualitative Research & Evaluation Methods. Sage.

[72]Braun, V., & Clarke, V. (2019). Reflecting on reflexive thematic analysis. Qualitative Research in Sport, Exercise and Health, 11(4), 589–597.

[73]Bryman, A. (2016). Social Research Methods. Oxford University Press.

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

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

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

[77] 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.

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

[79]Krosnick, J. A., & Presser, S. (2010). Question and Questionnaire Design. In Handbook of Survey Research (2nd ed., pp. 263–314). Emerald Group Publishing.

[80]DeVellis, R. F. (2017). Scale Development: Theory and Applications (4th ed.). Sage Publications.

[81]Hunyadi, L. & Vita, L. (2008). A kérdőíves vizsgálatok módszertana. Budapest: Aula Kiadó.

[82]Robson, C., & McCartan, K. (2016). Real World Research (4th ed.). Wiley.

[83] R. K. Ahuja, *Research Methods*, New Delhi: Rawat Publications, 2001.

[84] S. N. Hesse-Biber, *The Practice of Qualitative Research*, 3rd ed. London: SAGE Publications, 2016.

[85]Creswell, J. W., & Plano Clark, V. L. (2017). Designing and Conducting Mixed Methods Research. Sage.

[86] Small, M. L. (2009). ‘How many cases do I need?’ On science and the logic of case selection in field-based research. Ethnography, 10(1), 5–38.

[87] Flick, U. (2018). An Introduction to Qualitative Research (6th edition). Sage.

[88] 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.

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

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

[91] 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.

[92] C. Riessman, *Narrative Methods for the Human Sciences*, Thousand Oaks: Sage, 2008.

[93] J. Corbin and A. Strauss, *Basics of Qualitative Research*, 3rd ed. Thousand Oaks, CA: SAGE Publications, 2008.

[94] S. Yang, Y. Chen, Z. Song, et al., “Automotive Cybersecurity: A Survey on Frameworks, Standards, and Testing and Monitoring Technologies,” Sensors, vol. 24, no. 18, p. 6139, 2024.

[95] G. T. Ho, D. S. Wang, et al., “Security Analysis of In-Vehicle Networks and Protocols,” Vehicular Communications, vol. 43, p. 100639, 2023.

[96] A. Velinov, A. Mileva, S. Wendzel, W. Mazurczyk, “Covert Channels in the MQTT-based Internet of Things,” IEEE Access, vol. 7, pp. 161899–161915, 2019.

[97] H. S. Kim, H. Lee, et al., “Security and Privacy of MQTT and CoAP Protocols for the Internet of Things,” Wireless Networks, vol. 28, pp. 3221–3240, 2022.

[98] I. Ghafir, K. Prenosil, et al., “A Survey of IoT Protocols Security: MQTT, CoAP, AMQP and Beyond,” Wireless Networks, vol. 29, pp. 4921–4940, 2023.

[99] A. Shostack, Threat Modeling: Designing for Security, Wiley, 2014.

[100] B. Mosayyebpour, S. Ebrahimi, “Performance of Cryptographic Algorithms for Secure MQTT and HTTP Communications in IoT,” Information Systems Frontiers, vol. 25, pp. 965–982, 2023.

[101] S. Zander, G. Armitage, P. Branch, "A Survey of Covert Channels and Countermeasures in Computer Network Protocols," IEEE Communications Surveys & Tutorials, vol. 9, no. 3, pp. 44–57, 2007.

[102] A. Velinov et al., "Covert Channels in the MQTT-based Internet of Things," IEEE Access, vol. 7, pp. 161899–161915, 2019.

[103] B. Molnár, A. Csábrági, B. Forstner, "Képadat-védelmi kockázatok a járműfedélzeti rendszerekben," Infokommunikáció és Jog, vol. 18, no. 2, pp. 30–39, 2021.

[104] R. Togneri, D. Pullella, "An Overview of Speaker Identification: Accuracy, Robustness and Security," IEEE Circuits and Systems Magazine, vol. 11, no. 2, pp. 23–61, 2011.

[105] S. Mosaad, H. Hamza és I. A. Saroit, “Coverage in Mobile Wireless Sensor Networks (M-WSN): A Survey,” Computer Communications, vol. 110, pp. 1–13, 2017.

[106] J. Liu, G. Yue, S. Shen, H. Shang és H. Li, “Coverage Capacity Optimization for Mobile Sensor Networks Based on Evolutionary Games,” Mathematical Problems in Engineering, vol. 2014, Article ID 264307, 2014.

[107] V. S. Batista et al., “On the Coverage of Bus-Based Mobile Sensing,” Sensors (Basel), vol. 18, no. 6:1976, 2018.

[108] Q. Salman et al., “Vehicular Sensor Networks: Applications, Advances and Challenges,” Sensors, vol. 20, no. 13, Article 3686, 2020.

[109] Kiberbiztonság a XXI. században, 1. kiadás, Budapest: Akadémiai Kiadó, 2023.

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

[111] 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.

[112] 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.

[113] 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. URL: https://aisel.aisnet.org/icis2022/proceedings/Privacy/3/. (Letöltve: 2024.11.17.)

[114] F. Ahmed, S. Sen, and R. Khan, “Cybersecurity Challenges in Automotive Industry: A Survey,” Sensors, vol. 22, no. 6, 2022.

[115] INCIBE-CERT, “Keys for Implementing New Vehicle Cybersecurity Regulations: R155 and R156,” 2023.

[116] G. L. Beretta, “Cybersecurity risk assessment in automotive industry,” CNR ITIA, 2023.

[117] M. Khodadadi et al., “A Comparative Analysis of UNECE WP.29 R155 and ISO/SAE 21434,” ResearchGate, 2022.

[118] Trustonic, “Compliance with UNECE R155 and R156: What OEMs Need to Know,” Whitepaper, 2023.

[119] M. Heidl, S. Pillokat, and F. Kargl, “Cybersecurity Management System Evaluation Based on WP.29 R155,” in Lecture Notes in Computer Science, vol. 14333, 2023.

[120] European Commission, "Proposal for a Regulation on horizontal cybersecurity requirements for products with digital elements and amending Regulation (EU) 2019/1020," COM(2022) 454 final.

[121] European Union Agency for Cybersecurity (ENISA), "Cybersecurity requirements for connected devices," 2023.

[122] UNECE, "UN Regulation No. 155 on Cybersecurity and Cybersecurity Management System," 2021.

[123] European Commission, "Cyber Resilience Act - Questions and Answers," 2023.

[124] F. Weishäupl et al., “Cybersecurity in automotive supply chains: a layered responsibility,” Journal of Cybersecurity, vol. 8, no. 1, 2022.

[125] J. Hiller and R. Bélanger, “Data protection by design and the GDPR: A critical perspective,” Computer Law & Security Review, vol. 38, 2020.

[126] M. Abouelnaga and C. Jakobs, “Security Risk Analysis Methodologies for Automotive Systems,” arXiv preprint arXiv:2307.02261, 2023.

[127] T. Holz et al., “Systematization of Cybersecurity Requirements for Vehicles,” IEEE Security & Privacy, vol. 19, no. 4, pp. 50–57, 2021.

[128] European Journal of Risk Regulation, "Understanding the Regulatory Approach of the Cyber Resilience Act: Protection of Fundamental Rights in Disguise," Cambridge University Press, 2024.

[129] Computers & Security, "Cybersecurity regulation and compliance challenges in Europe," ScienceDirect, 2024.

[130] Wikipedia, "Cyber Resilience Act," 2024. [CRAOnline

[131] Lawfare, "The Cyber Resilience Act: An Accidental European Alien Torts Statute," 2024.

[132] Hogan Lovells, "The EU Cyber Resilience Act: Implications for Companies," 2024.

[133] elbilstatistikk.no, “Total cars registered,” Aug. 2025. [Online. Available: https://elbilstatistikk.no/

[134] “Norway celebrates another record year for electric vehicles,” elbil.no, Jan. 8, 2025. [Online. Available: https://elbil.no/fossil-fuel-cars-out-of-the-top-ten-list/

[135] J. Wehrman, “EVs At 23.5% Share In France — Plugins Dip As HEVs Surge,” CleanTechnica, Nov. 2, 2024. [Online. Available: https://cleantechnica.com/2024/11/02/evs-at-23-5-share-in-france-plugins-dip-as-hevs-surge/

[136] “Automotive OEM Telematics Research Report 2024–2030: Cars Sold in 2023 were Equipped with Embedded Telematics System,” Research and Markets via Globe Newswire, 01-Oct-2024. [Online. Available: https://rss.globenewswire.com/de/news-release/2024/10/01/2955832/28124/en/Automotive-OEM-Telematics-Research-Report-2024-2030-3-4-Cars-Sold-in-2023-were-Equipped-with-Embedded-Telematics-System-Apple-CarPlay-and-Android-Auto-Driving-Uptake-of-Smartphone-.html

[137] “Automakers are sharing consumers’ driving behavior with insurance companies,” Alpha Leaders, 2022. [Online. Available: https://alphaleaders.co.uk/automakers-are-sharing-consumers-driving-behavior-with-insurance-companies/

[138] “Automakers May Be Sharing Your Driving Data With Insurance Brokers,” InsideEVs.com, 2024. [Online. Available: https://insideevs.com/news/712079/automakers-insurance-data-brokers-criticalmaterials/

[139] Tavakol, M., & Dennick, R. (2011). Making sense of Cronbach's alpha. International journal of medical education, 2, 53–55.

[140] Guttman, L. (1945). A basis for analyzing test-retest reliability. Psychometrika, 10(4), 255–282.

[141] Mahalanobis, P. C. (1936). On the generalised distance in statistics. Proceedings of the National Institute of Sciences of India, 2(1), 49–55.

[142] European Data Protection Supervisor, "TechDispatch #3: Connected Cars," 2020. [NKOnline

[143] A. Khan et al., "Data Privacy and Security in Autonomous Connected Vehicles in Smart City Environment," Drones, vol. 8, no. 9, 2023.

[144] S. Brown et al., "Evaluating Consumer Understanding and Awareness of Connected and Autonomous Vehicle Data Privacy," in Responsible Design, Implementation and Use, Springer, 2023.

[145] R. Harrison et al., "Privacy preferences in automotive data collection," Technology in Society, vol. 76, 2024.

[146] Smith, J., Brown, L., & Garcia, P. (2022). Security Threats in Connected Vehicles. IEEE Access, 10, 23456–23468.

[147] Müller, K., Zhang, Y., & Patel, S. (2023). Data Leakage via In-Vehicle Communication: Risks and Prevention. Computers & Security, 120, 102834.

[148] Shin, D., & Park, Y. (2021). Understanding the Attitudes of Consumers Toward Smart Car Data Privacy: An Empirical Study. Telematics and Informatics, 63, 101651.

[149] 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.

[150] 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.

[151] M. Wolf, A. Weimerskirch, C. Paar, "Security in Automotive Bus Systems," Proc. IEEE, vol. 95, no. 2, pp. 387-399, 2007.

[152] P. Kleberger, T. Olovsson, E. Jonsson, "Security Aspects of the In-Vehicle Network in the Connected Car," in Intelligent Vehicles Symposium, 2011.

[153] P. Papadimitratos et al., "Secure Vehicular Communication Systems: Design and Architecture," IEEE Commun. Mag., vol. 46, no. 11, 2008.

[154] KPMG, "Connected and Autonomous Vehicles: The UK Economic Opportunity," White Paper, 2019.

[155] T. Hoppe, S. Kiltz, J. Dittmann, "Security Threats to Automotive CAN Networks—Practical Examples and Selected Short-Term Countermeasures," Reliab. Eng. Syst. Saf., vol. 96, no. 1, pp. 11-25, 2011.

[156] J. Petit, S. E. Shladover, "Potential Cyberattacks on Automated Vehicles," IEEE Trans. Intell. Transp. Syst., vol. 16, no. 2, 2015.

[157] D. Klinedinst, K. Park, "Hacking Connected Cars: Tactics, Techniques, and Procedures," Carnegie Mellon CERT Report, 2017.

[158] S. Checkoway et al., "Comprehensive Experimental Analyses of Automotive Attack Surfaces," in USENIX Security Symposium, 2011.

[159] ENISA, "Good Practices for Security of Smart Cars," European Union Agency for Cybersecurity, 2019.

[160] J. C. Bazydlo et al., "Connected Vehicles and Privacy: A Policy Perspective," Telematics and Informatics, vol. 65, 2022.

[161] A. Greenberg, "Hackers Remotely Kill a Jeep on the Highway—With Me in It," Wired, 2015.

[162] H. Boyes, "Security, Privacy, and Connected Vehicles," IET Intelligent Transport Systems, vol. 11, no. 3, pp. 164-170, 2017.

[163] Reuters, "Tesla workers shared sensitive images recorded by customer cars," Reuters Investigates, 2023.

[164] G. Loukas, Cyber-Physical Attacks: A Growing Invisible Threat, Elsevier, 2015.

[165] M. S. Fareed, M. Qureshi, "Security Challenges in Automotive Embedded Networks: A Survey," IEEE Access, vol. 8, pp. 212004-212029, 2020.

[166] H. Debar, E. Filiol, "Telematics and Privacy: Usage-Based Insurance and Data Protection," in Vehicular Communications and Networks, Wiley, 2022.

[167] T. Neudecker et al., "Privacy Risks in Connected Car Data Sharing," IEEE Security & Privacy, vol. 19, no. 2, pp. 31-39, 2021.

[168] G. N. Ericsson, "Cyber Security and Power System Communication—Essential Parts of a Smart Grid Infrastructure," IEEE Trans. Power Del., vol. 25, no. 3, pp. 1501-1507, 2010.

[169] T. Holz et al., "Internet of Vehicles: Security and Privacy Issues," in IEEE International Symposium on Circuits and Systems (ISCAS), 2017.

[170] ENISA, "Cybersecurity Challenges in the Upstream Oil and Gas Sector," 2019.

[171] C. Miller, C. Valasek, "Remote Exploitation of an Unaltered Passenger Vehicle," Black Hat USA, 2015.

[172] E. Ronen, A. Shamir, "Extended Functionality Attacks on IoT Devices: The Case of Smart Lights," in IEEE European Symposium on Security and Privacy, 2017.

[173] N. Paladi, "Security Analysis of OTA Updates in the Automotive Industry," Springer Automotive Series, 2019.

[174] A. Greenberg, "Automotive Security: IP Protocols in Modern Vehicles," Wired, 2017.

[175] S. T. Ali, A. A. Ghorbani, "On the Use of IoT Protocols in the Automotive Sector," IoT Security Review, vol. 4, no. 2, 2021.

[176] S. Yin, "The Application of OSI Model in Automotive Communication Systems," IEEE Vehicular Technology Magazine, vol. 16, no. 2, pp. 89-94, 2021.

[177] R. Bosch, Automotive Handbook, 10th ed., Wiley, 2023.

[178] P. H. Chavan et al., "Automotive Cybersecurity: A Review of Protocols, Threats, and Testbeds," IEEE Access, vol. 10, pp. 78469-78498, 2022.

[179] G. Velinov, F. Turuk, "Security Analysis of MQTT and CoAP Protocols for IoT-based Smart Vehicles," IEEE Access, vol. 10, 2022.

[180] B. Groza et al., "Security of the Internet of Vehicles: Communication Protocols, Attacks, and Countermeasures," IEEE Communications Surveys & Tutorials, vol. 24, no. 1, pp. 175-200, 2022.

[181] P. Kietzmann et al., "A Security Analysis of MQTT Protocol in Automotive IoT," in IEEE IoT World Forum, 2021.

[182] S. Mallouhi et al., "Cyber Attack Modeling Analysis for SCADA Systems," Proc. International Conference on Critical Infrastructure Protection, 2011.

[183] S. Bhunia, M. Tehranipoor, Hardware Security: A Hands-on Learning Approach, Elsevier, 2019.

[184] O. Hohlfeld, A. Feldmann, "Internet of Things—Communication Protocols and Security Issues," ACM Computing Surveys, vol. 54, no. 1, 2021.

[185] AUTOSAR, "SecOC—Secure Onboard Communication," AUTOSAR Release 4.7, 2021.

[186] J. B. Kenney, "Dedicated Short-Range Communications (DSRC) Standards in the United States," Proc. IEEE, vol. 99, no. 7, 2011.

[187] M. Khari et al., "Critical Review of Security Threats in the Internet of Vehicles," IEEE Access, vol. 8, 2020.

[188] J. Kim et al., "Analysis of Security Vulnerabilities in the CoAP Protocol," Sensors, vol. 21, no. 13, 2021.

[189] R. Singh et al., "A Study of MQTT Protocol in Connected Vehicle Scenarios," in IEEE International Conference on IoT, 2019.

[190] S. Ghafir et al., "Security Threats to the MQTT Protocol in Connected Cars," Journal of Cyber Security Technology, vol. 7, no. 3, 2023.

[191] J. Kim et al., "Security Analysis of CoAP Protocol for IoT-based Vehicles," Sensors, vol. 19, no. 6, 2019.

[192] D. Puschmann et al., "Security Analysis of CoAP Communication in Vehicle Networks," IEEE Vehicular Technology Conf., 2022.

[193] R. Fielding, "Architectural Styles and the Design of Network-based Software Architectures," PhD Dissertation, UC Irvine, 2000.

[194] S. H. Lee and H. Jeong, "HTTPS and API Security in Automotive Environments," IEEE Access, vol. 10, pp. 53521-53536, 2022. doi: 10.1109/ACCESS.2022.3176956

[195] S. Mazloom, M. A. Azgomi, and R. Ebrahimi Atani, "Security Analysis of TLS Implementations in Automotive Systems," in 2021 10th International Conference on Computer and Knowledge Engineering (ICCKE), 2021, pp. 53-58. doi: 10.1109/ICCKE52421.2021.9613642

[196] R. Hussain, S. A. Idrees, and S. Kim, “Autonomous vehicles and connected cars—current status and future perspectives,” Elsevier Vehicular Communications, vol. 29, p. 100418, 2021.

[197] G. Preuveneers, A. Ilie-Zudor, “The intelligent industry of the future: A survey on emerging technologies, applications and open research topics,” Computers in Industry, vol. 123, p. 103334, 2020.

[198] S. Raza, L. Wallgren, and T. Voigt, “Security Considerations for the RESTful Web Services with CoAP,” Proc. IEEE Int. Conf. on Communications (ICC), 2013.

[199] J. Soldatos, “How the MQTT Protocol Works and Why It Matters for IoT,” IEEE Internet of Things Magazine, vol. 3, no. 4, pp. 43–47, 2020.

[200] M. S. Abualhassan et al., “Security Analysis of the MQTT Protocol in the Internet of Things (IoT),” Sensors, vol. 23, no. 2, 2023.

[201] S. Kim, J. Kim, J. Jang, “Analysis of Automotive OTA Communication Protocols for Secure Software Updates,” IEEE Access, vol. 9, pp. 167233–167249, 2021.

[202] L. Apvrille, “Cybersecurity Challenges in the Automotive Domain,” IEEE Design & Test, vol. 38, no. 1, pp. 7–17, 2021.

[203] I. Ghafir, F. Prenafeta-Boldú, M. Hammoudeh, “Security of MQTT Protocol in Smart Connected Vehicles: A Review,” IEEE Access, vol. 10, pp. 11719–11732, 2022.

[204] K. Hartke, “Observing Resources in CoAP,” IETF RFC 7641, 2015.

[205] R. C. A. Alves et al., “A Survey on CoAP Protocol: Security, Attacks, and Research Trends,” Journal of Network and Computer Applications, vol. 207, p. 103530, 2022.

[206] R. Droms et al., “Security in Embedded and Automotive Networks,” IEEE Transactions on Dependable and Secure Computing, vol. 18, no. 2, pp. 611–624, 2021.

[207] R. Ahmad et al., “A Comprehensive Analysis of TLS/DTLS for the Internet of Things,” IEEE Access, vol. 7, pp. 135788–135804, 2019.

[208] M. B. Santos et al., “IoT Security Attacks and Countermeasures in Automotive Environments: A Review,” IEEE Access, vol. 10, pp. 3883–3902, 2022.

[209] A. Velinov, B. Rajšl, M. Zajc, “Over-the-Air Communication Security in Connected Vehicles,” IEEE Access, vol. 8, pp. 121423–121436, 2020.

[210] J. P. Vilela et al., “Covert Channels in Security Protocols: A Survey,” IEEE Communications Surveys & Tutorials, vol. 22, no. 2, pp. 1098–1136, 2020.

[211] I. Ghafir, R. Islam, “Application-Layer Attacks on IoT Protocols: A Survey,” IEEE Access, vol. 10, pp. 3427–3452, 2022.

[212]H. Hegyi, "A személygépjárművek információbiztonsága az információbiztonsági szakértők szemszögéből," Biztonságtudományi Szemle, vol. 5, no. 2, pp. 47–58, 2023.

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

[214] Bendix- Service data for ABS, URL:https://n0c357rmy1njbuit2friqwu.blob.core.windows.net/documents/U3eJunINI0EBhB_SD-13-4746_US_000.pdf

[215] Autorepair, Decoding Vehicle Diagnostics: What Your Car Is Trying to Tell You URL: https://allaroundautorepair.com/understanding-traction-control-and-abs-systems-history-functionality-and-failure-implications

[216] Bosch - Electronic Stability Program, URL:https://www.bosch-mobility.com/en/solutions/driving-safety/electronic-stability-program/

[217] 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.

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

[219] 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.

[220] 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.

[221] 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).

[222] 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.

[223] 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.

[224]C. Jemine, “Automatic multispeaker voice cloning,” M.S. thesis, Univ. of Liège, Liège, Belgium, 2019. URL: https://matheo.uliege.be/handle/2268.2/6801 [Online

[225] The Intercept, “American phone-tracking firm demoed surveillance powers by spying on CIA and NSA”

[226] M. Raciti & G. Bella, “Up-to-date Threat Modelling for Soft Privacy on Smart Cars”, arXiv, 2023.

[227] AP News, “Biden orders US investigation of national security risks posed by Chinese-made ‘smart cars’”, 2023.

[228] Electropages, “Security Risks of Smart Cars”, 2024.

[229] J. Lewis, “Connected Cars and Spying”, CSIS, 2024.

[230] The Guardian, “Are electric cars vulnerable to cyber spies…”, 2025.

[231]F. Swiderski and W. Snyder, Threat Modeling. Redmond, WA: Microsoft Press, 2004.

[232] R. J. Creemers, "China’s emerging data protection framework," Journal of Cybersecurity, vol. 8, no. 1, tyac011, 2022. [Online. Available: https://www.researchgate.net/publication/362915856_China%27s_emerging_data_protection_framework

[233] Law.asia, "Data compliance according to China’s automotive industry," Aug. 13, 2024. [Online. Available: https://law.asia/china-automotive-industry-data-compliance/

[234] "Personal Information Protection Law of the People’s Republic of China," Wikipedia. [Online. Available: https://en.wikipedia.org/wiki/Personal_Information_Protection_Law_of_the_People%27s_Republic_of_China

[235] "Data Security Law of the People’s Republic of China," Wikipedia. [Online. Available: https://en.wikipedia.org/wiki/Data_Security_Law_of_the_People%27s_Republic_of_China

[236] "Cybersecurity Law of the People’s Republic of China," Wikipedia. [Online. Available: https://en.wikipedia.org/wiki/Cybersecurity_Law_of_the_People%27s_Republic_of_China

[237] National Highway Traffic Safety Administration, "Cybersecurity Best Practices for the Safety of Modern Vehicles," DOT HS 812 333, 2021. [Online. Available: https://www.nhtsa.gov/sites/nhtsa.gov/files/documents/812333_cybersecurityformodernvehicles.pdf

[238] National Institute of Standards and Technology, "Security and Privacy Controls for Information Systems and Organizations," NIST SP 800-53 Rev. 5, 2020. [Online. Available: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r5.pdf

[239] JASPAR, "Automotive Cybersecurity Guidelines," JASPAR Association, 2023. [Online. Available: https://www.jaspar.jp/en/activities/cybersecurity/

[240] United Nations Economic Commission for Europe, "UNECE Regulation No. 155 - Cyber security and cyber security management system," 2021. [Online. Available: https://unece.org/transport/vehicle-regulations/wp29/standards/cybersecurity

[241] European Parliament and Council, "Directive (EU) 2022/2555 on measures for a high common level of cybersecurity across the Union (NIS2)," Dec. 2022. [Online. Available: https://eur-lex.europa.eu/eli/dir/2022/2555/oj

[242] European Union Agency for Cybersecurity (ENISA), "Good practices for security of Smart Cars," 2021. [Online. Available: https://www.enisa.europa.eu/publications/good-practices-for-security-of-smart-cars

[243] European Commission, "Cyber Resilience Act," 2022. [Online. Available: https://digital-strategy.ec.europa.eu/en/policies/cyber-resilience-act

[244] S. Gürses, R. van Hoboken, "Privacy after the Agile Turn: Governance, Design, and the Limits of Privacy by Design," Fordham Law Review, vol. 88, no. 2, pp. 437–468, 2019.

[245] P. M. Schwartz, "Global Data Privacy: The EU Way," NYU Law Review, vol. 94, pp. 771–818, 2019.

[246] R. Leenes, R. van Brakel, S. Gutwirth, P. De Hert (eds.), "Data Protection and Privacy: (In)visibilities and Infrastructures," Springer, 2017.

[247] Y. Wang, Y. Wang, H. Qin, and J. Wang, “A Systematic Risk Assessment Framework of Automotive Cybersecurity,” Automotive Innovation, vol. 4, pp. 253–261, 2021. [Online. Available: https://link.springer.com/article/10.1007/s42154-021-00140-6

[248] F. Luo, Y. Jiang, J. Wang, Z. Li, and X. Zhang, “A Framework for Cybersecurity Requirements Management in the Automotive Domain,” Sensors, vol. 23, no. 10, 4979, 2023. [Online. Available: https://www.mdpi.com/1424-8220/23/10/4979

[249] ENISA, "Cybersecurity for Connected and Automated Mobility," European Union Agency for Cybersecurity, 2021. [Online. Available: https://www.enisa.europa.eu/publications/cybersecurity-for-connected-and-automated-mobility

[250] S. Gürses, R. van Hoboken, "Privacy after the Agile Turn: Governance, Design, and the Limits of Privacy by Design," Fordham Law Review, vol. 88, no. 2, pp. 437–468, 2019. [Online. Available: https://ir.lawnet.fordham.edu/flr/vol88/iss2/3/

[251] P. M. Schwartz, "Global Data Privacy: The EU Way," NYU Law Review, vol. 94, pp. 771–818, 2019. [Online. Available: https://www.nyulawreview.org/issues/volume-94-number-4/global-data-privacy-the-eu-way/

[252] R. Leenes, R. van Brakel, S. Gutwirth, P. De Hert (eds.), "Data Protection and Privacy: (In)visibilities and Infrastructures," Springer, 2017. [Online. Available: https://link.springer.com/book/10.1007/978-3-319-50796-9

[253] European Commission, "Proposal for a Regulation on horizontal cybersecurity requirements for products with digital elements (Cyber Resilience Act)," 2022. [Online. Available: https://digital-strategy.ec.europa.eu/en/library/cyber-resilience-act-proposal-and-factsheets

[254] Y. Wang, Y. Wang, H. Qin, and J. Wang, “A Systematic Risk Assessment Framework of Automotive Cybersecurity,” Automotive Innovation, vol. 4, pp. 253–261, 2021. [Online. Available: https://link.springer.com/article/10.1007/s42154-021-00140-6

[255] F. Luo, Y. Jiang, J. Wang, Z. Li, and X. Zhang, “A Framework for Cybersecurity Requirements Management in the Automotive Domain,” Sensors, vol. 23, no. 10, 4979, 2023. [Online. Available: https://www.mdpi.com/1424-8220/23/10/4979

[256]N. Shiwakoti, P. Stasinopoulos, Y. Chen, and M. Warren, “Cybersecurity framework for connected and automated vehicles: A modelling perspective,” Transport Policy, vol. 162, pp. 47–64, 2025. [Online

[257] A. Alfardus and D. B. Rawat, "Machine Learning-Based Anomaly Detection for Securing In-Vehicle Networks," Electronics, vol. 13, no. 10, 1962, 2024. [Online. Available: https://www.mdpi.com/2079-9292/13/10/1962

[258] A. Gupta, S. Tiwari, R. Tripathi, and P. K. Singh, "Detecting Cyber Attacks In-Vehicle Diagnostics Using an Intelligent Multistage Framework," Sensors, vol. 23, no. 18, 7941, 2023. [Online. Available: https://www.mdpi.com/1424-8220/23/18/7941

[259] A. Aloqaily, M. Abdallah, T. R. Sheltami, and I. A. Al Ridhawi, "Supervised Machine Learning for Real-Time Intrusion Attack Detection in Connected and Autonomous Vehicles: A Security Paradigm Shift," Informatics, vol. 12, no. 1, 4, 2025. [Online. Available: https://www.mdpi.com/2227-9709/12/1/4]

12.MELLÉKLETEK

1. Számú melléklet – A kínai gyártók térnyerésének számszerűsített adatai

A táblázat az egyes gyártók típusonkénti értékesítési arányait, összesített darabszámát és az előző évhez viszonyított változást mutatja be, külön kiemelve a kínai tulajdonú vállalatokat. A kimutatás jól szemlélteti, hogy a kínai szereplők nemcsak a volumen, hanem a hajtáslánc-technológiák diverzifikációja terén is egyre erőteljesebb pozíciót foglalnak el az európai piacon.

Helye-zés	Gyártó	Belső égésű (%)	Elektromos (BEV) (%)	Hibrid (HEV) (%)	Plug-in hibrid (PHEV) (%)	Egyéb (%)	Darabszám	Változás (előző évhez képest)
1	Volkswagen Csoport	68	20	0	10	1	303268	3%
2	Stellantis	83	13	0	3	2	168867	-3%
3	Renault Csoport	58	11	30	1	1	109712	5%
4	Hyundai-Kia	54	20	18	7	1	88401	-1%
5	BMW Csoport	61	24	0	15	0	78231	6%
6	Toyota	14	5	72	9	0	76537	-4%
7	Mercedes-Benz	65	14	0	20	1	58442	2%
8	Ford	62	18	8	12	1	41110	9%
9	Geely Csoport	31	38	0	30	1	32992	-11%
10	SAIC	42	15	34	9	0	29387	30%

11. táblázat - Kína gyártók térnyerése. Forrás: JATO[10].

[10] JATO: Kínai gyártók térnyerése. URL: https://www.jato.com/resources/media-and-press-releases/chinese-automakers-double-european-market-share-in-may (letöltve: 2025.08.05.)

2. Számú melléklet – Definíciós táblázatok

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 [48].	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 [44], [45].

12. táblázat - Az internethez csatlakozó személygépjárművek két típusa a csatlakozás módja szerint. Forrás: saját forrás.

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 [49].	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 [50].

13. táblázat - Az okosautó és az internetkapcsolatra képes autó definíciós különbségei. Forrás: saját forrás.

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 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.	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, 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.

14. táblázat - Az adatvédelem és adatbiztonság fogalmi megkülönböztetése. Forrás: saját forrás.

Forrás	Definíció
NIST SP 1800-16B-C	Eszközök hálózata, amely tartalmazza a hardvert, szoftvert és firmware-t, illetve azokat a komponenseket, amelyek lehetővé teszik az eszközök kapcsolódását, kölcsönhatását és szabad adat- és információcsere lehetőségét.[11]

[11] NIST SP 1800-16B-C. URL: https://csrc.nist.gov/glossary/term/internet_of_things (letöltve 2025.08.10)

Forrás	Definíció
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.[12]
Gartner	Az "Internet of Things" (IoT) a fizikai tárgyak hálózata, amelyek beépített technológiával rendelkeznek, hogy kommunikáljanak, érzékeljenek vagy kölcsönhatásba lépjenek a belső állapotukkal vagy a külső környezettel.[13]
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.[14]

15. táblázat - IoT definíciók. Forrás: saját forrás.

3. Számú melléklet - Főbb járműipari kiber- és információbiztonsági előírásokat jogi kötelező erejük, alkalmazási körük, felügyeleti mechanizmusuk és szankciórendszerük szerint

Szabvány vagy 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

[12] NIST SP 1800-16B-C. URL: https://csrc.nist.gov/glossary/term/internet_of_things (letöltve 2025.08.10)
[13] Gartner: Internet of Things Glossary. URL: https://www.gartner.com/en/information-technology/glossary/internet-of-things (2025.08.10)
[14] Európai Parlament: IoT. URL https://www.europarl.europa.eu/RegData/etudes/BRIE/2015/557012/EPRS_BRI(2015)557012_EN.pdf (letöltve: 2025.08.10)

Szabvány vagy Jogszabály	Elterjedtség	Kötelező?	Érintettek	Felügyelet	Szankciók
CRA	Új EU-s jogszabály, 2025-től került elfogadásra, 2027-től alkalmazandó.	Igen, kötelező lesz minden digitális terméket és szoftvert előállító vagy forgalmazó cég számára az EU piacán.	Autógyártók, szoftverfejlesztők, beszállítók, bármely digitális elemet tartalmazó termék gyártói.	Nemzeti piacfelügyeleti hatóságok és az EU kiberbiztonsági ügynöksége (ENISA) közreműködhet.	Pénzbírság akár a globális éves árbevétel 2,5%-áig, piacról való kitiltás, kötelező termékvisszahívás.
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

Szabvány vagy Jogszabály	Elterjedtség	Kötelező?	Érintettek	Felügyelet	Szankciók
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
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

16. táblázat - A szabályozási környezet értékelése - Átfogó vizsgálat. Forrás: saját forrás.

4. Számú melléklet – Az egyes szabványok főbb jellemzői és célkitűzései

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
CRA	Digitális termékek és szoftverek kiberbiztonsági megfelelősége	Kiberbiztonság	Beépített biztonság („security by design”), kockázatalapú megközelítés, kötelező sebezhetőség-kezelés, piacfelügyeleti megfelelés
ISO 26262	Funkcionális biztonság	Funkcionális biztonság	Funkcionális biztonsági követelmények, ASIL szintek

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

17. táblázat - A szabályozási környezet értékelése – Indexelés. Forrás: saját forrás.

5. Számú melléklet - Életciklus-alapú fenyegetéselemzés

Életciklus szakasz	Kapcsolódó támadástípusok	Magyarázat / Indoklás
Koncepció / Termékdefiníció	Supply chain, Privát adatok	Ebben a fázisban történik a specifikációk és beszállítók kiválasztása. Már ekkor is bekerülhetnek gyenge láncszemek vagy kockázatos partnerek, akik nem felelnek meg kiberbiztonsági követelményeknek. A specifikációs dokumentumok vagy partnerek kiszivárogtatása üzleti kárt is okozhat.
Tervezés / Architektúra kialakítása	Tárolt adatok, Firmware, CAN	A jármű rendszerarchitektúrájának kialakításakor eldől, hogyan oszlanak el az irányítási és kommunikációs funkciók. Ha a tervezés során nem gondolnak megfelelően a CAN-busz vagy firmware védelmére, strukturális sebezhetőségek keletkeznek.
Fejlesztés (szoftver, hardver)	Firmware, Supply chain, Backdoor (Távoli hozzáférés)	A fejlesztési fázisban kerülhet be kártékony kód vagy nem dokumentált "hátsó ajtó" (backdoor), akár szándékosan, akár hanyagságból. A nyílt forrású vagy harmadik féltől származó komponensek szintén kockázatot hordoznak.
Integráció / Tesztelés	Szenzor, CAN, Tárolt adatok	A komponensek integrálásakor és tesztelésekor kiderülhetnek inkompatibilitások, de a hiányos tesztelés révén rejtve is maradhatnak sebezhetőségek. A szenzorok manipulációja vagy hibakezelési hiányosságok is ezen a ponton detektálhatóak lennének, ha megfelelő tesztelési terv állna rendelkezésre.
Gyártás / Összeszerelés	Supply chain, Tárolt adatok	A végszerelés során is előfordulhat nem megfelelő vagy hamisított alkatrészek használata, amelyek sebezhetőséget hordoznak. A beégetett gyári adatok védelme kritikus.
Piacra lépés / Típusjóváhagyás	Távoli hozzáférés, Privát adatok	A jármű ekkor kerül forgalomba. A típusjóváhagyás során meg kellene vizsgálni a távoli frissítési képességeket, hozzáférési vektorokat, de ezek gyakran csak adminisztratív szinten kerülnek értékelésre.
Használat / Karbantartás	Bluetooth/Wi-Fi, Telematika, OTA, Ransomware	A jármű üzemeltetése során rengeteg adatot gyűjt (pl. vezetési stílus, helyadatok). A telematikai csatornák és OTA frissítések támadhatók, a Bluetooth vagy Wi-Fi kapcsolatokkal pedig jogosulatlan hozzáférést lehet

Életciklus szakasz	Kapcsolódó támadástípusok	Magyarázat / Indoklás
		szerezni. Céges járműflottáknál ransomware támadás is előfordulhat.
Selejtezés / Életciklus vége	Firmware, Tárolt adatok, Privát adatok	A járművek leselejtezésekor gyakran nem megfelelően törlik az adatokat. Ez visszaélésekhez vezethet, például korábbi tulajdonosok személyes adatainak megszerzéséhez. Az elavult szoftverek is visszafejthetők lehetnek később.

18. táblázat - Életciklus-alapú fenyegetéselemzés személygépjárművek esetén. Forrás: saját forrás.

6. Számú melléklet – SAW módszertanon alapú értékelési keret és a szabályozási környezet részletes vizsgálata

Hatóság, szankció, felügyelet - Pontozás	
Összpontszám:	3
Hatóság:	1
Szankció:	1
Felügyelet:	1

Támadások elleni védelem - Pontozás	
Összpontszám:	14
Zöld mezők:	2
Sárga mezők:	1
Piros mezők:	0

19. *táblázat - Hatóság, szankció, felügyelet és támadások elleni védelem pontozása. Forrás: saját forrás.*

Megfelelési skála																
		Támadások elleni védelem														
Hatóság, szankció, felügyelet	X	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14
	0	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14
	1	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
	2	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
	3	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17

20. *táblázat - A szabályozási és technikai megfelelés értékelési skálája. Forrás :saját forrás.*

Eredmények:	
0-4	Nem megfelelő
5-8	Alacsony erejű
9-12	Közepes erejű
13-16	Megfelelő
17	Ideális

21. *táblázat - Eredemények leképezése. Forrás: saját forrás.*

Szabályozás	Kötelező	Szankció	Felügyelet	Távoli elérés	Tárolt adatok	Szenzor	CAN	Firmware	Beszállítói lánc	Személyes adatok	Pont	Besorolás
ISO/SAE 21434	Nem kötelező	Nincsenek hivatalos szankciók	Nincs hivatalos felügyelet	✓ Részletes technikai elvárások, fókuszban a jármű. Nem kötelező, iparági elvárás.	✓ Kockázatok kezelésének része. Felhasználói adatokat csak közvetetten érinti.	△ Szenzorfúziós fenyegetések elemzése kötelező lehet, de mélységi vizsgálatot nem vár el.	△ Protokollszintű védelmet nem ír elő, de hálózati kockázatok elemzése elvárt.	✓ Szoftverek integritására kitér, bár nem mély technikai szinten.	△ Elvileg megköveteli a beszállítók auditját, de nincsen kényszerítő hatóság mögötte. A beszállítókra közvetlenül nem vonatkozik.	✗ Nem elsődleges cél.	**9**	**Közepes erejű**
UNECE WP.29 – R155, R156	Kötelező	Típusjóváhagyás megtagadása, forgalmazás kizárása	Nemzeti közlekedési hatóságok	✓ Kötelező a kiberbiztonsági menedzsment rendszer (CSMS). Hatóság ellenőrzi.	✓ Védi a kritikus adatok integritását és titkosságát.	△ Kevéssé tárgyalja. Elsősorban hálózati és szoftveres kockázatokat vizsgál.	✓ R155 keretrendszere alapján elvárt a CAN manipulációval szembeni védelem. (TARA módszertan)	✓ R156 szoftverfrissítés-menedzsmentet ír elő. Hatóságilag számonkérhető jogszabály.	△ Az R155 előírja a beszállítók bevonását a CSMS-be. Kiemelten kezelt terület, de a gyakorlatban a beszállítótól függ, hogy átadja-e az adatokat, mivel rájuk közvetlenül semmilyen előírás nem vonatkozik.	✗ Nem elsődleges cél.	**13**	**Megfelelő**
ISO 26262	Nem mindenhol kötelező	OEM kizárhatja a beszállítót	Nincs közvetlen hatósági felügyelet	✗ Funkcionális biztonságra fókuszál, nem számítógépes támadásokra.	✗ Nem foglalkozik vele.	✓ Szenzorhibák, szenzorfúzió biztonsági elemzése kötelező. Jó lefedettség.	△ Kommunikációs hibákra van eljárás, de nem támadás elleni védelem.	△ Szoftverhibák szempontjából elemzi, de nem részletesen az ellenséges manipulációra.	✗ Beszállítókat nem biztonsági szemszögből kezeli.	✗ Nem célja a felhasználói védelem.	**4**	**Nem megfelelő**
ISO/IEC 27001	Nem kötelező az autóiparban	Nincsenek jogi szankciók, de reputációs hátrány, piacvesztés lehet	Szabvány szerinti auditálás	✓ IT rendszerek hozzáférés-kezelését szabályozza, de nem specifikus járművekre.	✓ Adatvédelem, titkosítás, hozzáférés – részletes.	✗ Nem vonatkozik fizikai érzékelőkre.	✗ Nem specifikus.	△ Szerver oldali firmware-kezelés lehet benne, de nem járműspecifikus.	△ Szállítói kockázatok kezelésének része, de az eredmény és mélység nagyban függ a szállító közreműködésétől.	✓ Védi a személyes és üzleti adatokat – vállalati fókusszal.	**8**	**Közepes erejű**

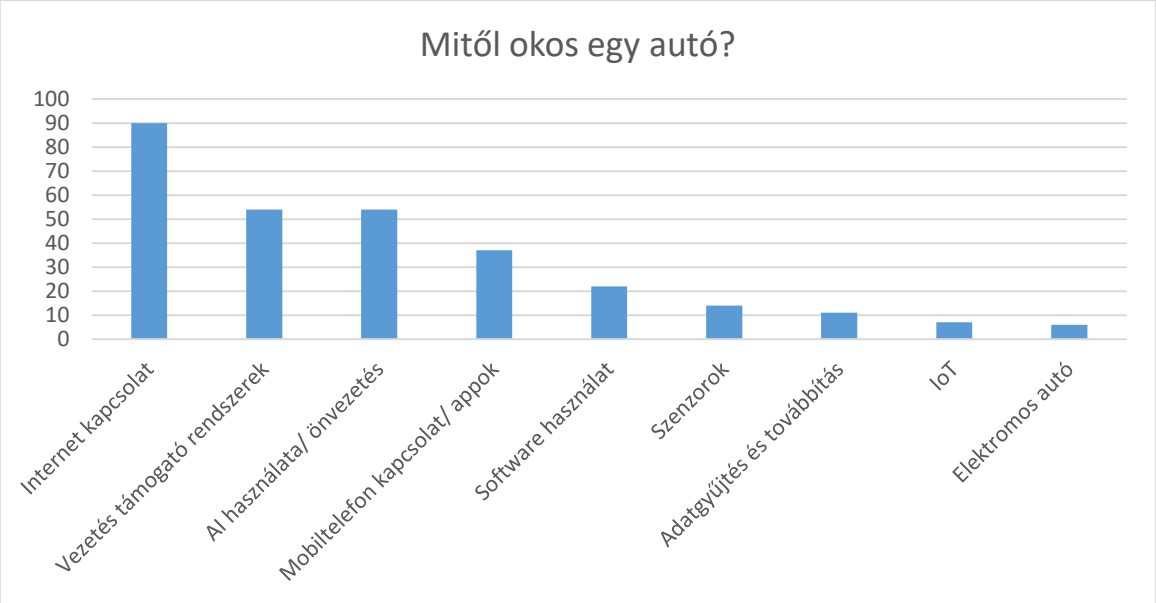
Szabályozás	Kötelező	Szankció	Felügyelet	Távoli elérés	Tárolt adatok	Szenzor	CAN	Firmware	Beszállítói lánc	Személyes adatok	Pont	Besorolás
NIST Cybersecurity Framework	Nem kötelező	Nincsenek jogi szankciók, de reputációs hátrány, piacvesztés lehet	Nincs közvetlen hatósági felügyelet	✓ Ernyő jellegű keretrendszer. Nem specifikus, de jó gyakorlati alap.	✓ Része a védelmi, észlelési, helyreállítási funkcióknak.	✗ Nem foglalkozik vele.	✗ Nem érinti közvetlenül.	△ Firmware-kezelés lehet az 'Identify' és 'Protect' része.	△ Szállítói kockázatkezelés része, de az eredmény és mélység nagyban függ a szállító közreműködésétől.	✓ Tartalmaz adatvédelmi szempontokat	**8**	**Közepes erejű**
AUTOSAR Adaptive Platform	Nem kötelező	Nincsenek hivatalos szankciók	AUTOSAR konzorcium	△ Technológiai alapot nyújt, de nem szabályozza a védelmi intézkedést.	✗ Nem tárgyalja ezt a területet.	✗ Nem tárgyalja ezt a területet.	✗ Nem tárgyalja ezt a területet.	✓ Architektúra és fejlesztési folyamat szintjén támogatja a biztonságos implementációt.	✓ Architektúra és fejlesztési folyamat szintjén támogatja a biztonságos implementációt.	✗ Nem tárgyalja ezt a területet.	**6**	**Alacsony erejű**
ISO/IEC 15408 (Common Criteria)	Nem kötelező	Nincsenek jogi szankciók, de reputációs hátrány, piacvesztés lehet	Nemzeti kormányok tanúsítása	✓ Biztonsági célok és értékelési szintek mentén vizsgálható, részletes, de nem specifikus.	✓ Biztonsági célok és értékelési szintek mentén vizsgálható, részletes, de nem specifikus.	✗ Nem releváns ebben a kontextusban.	✗ Nem releváns ebben a kontextusban.	✗ Nem releváns ebben a kontextusban.	✗ Nem releváns ebben a kontextusban.	✓ Biztonsági célok és értékelési szintek mentén vizsgálható, részletes, de nem specifikus.	**6**	**Alacsony erejű**
ISO 24089	Nem kötelező	OEM kizárhatja a beszállítót	Nincs közvetlen felügyelet	✗ Kizárólag a szoftverek frissítésére fókuszál.	✗ Kizárólag a szoftverek frissítésére fókuszál.	✗ Kizárólag a szoftverek frissítésére fókuszál.	✗ Kizárólag a szoftverek frissítésére fókuszál.	✓ Szoftverek frissítésének életciklusának kezelését szabályozza.	✗ Kizárólag a szoftverek frissítésére fókuszál.	✗ Kizárólag a szoftverek frissítésére fókuszál.	**2**	**Nem megfelelő**

Szabályozás	Kötelező	Szankció	Felügyelet	Távoli elérés	Tárolt adatok	Szenzor	CAN	Firmware	Beszállítói lánc	Személyes adatok	Pont	Besorolás
CRA	Kötelező	Európai Bizottság, ENISA, nemzeti hatóságok	Igen, súlyos pénzbírságok	✓ Kiemelten szabályozza a hálózatra kapcsolt eszközök biztonságát, beleértve a távoli hozzáférési felületeket is. Kötelező a biztonsági frissítések biztosítása.	✓ Elvárás, hogy az eszközök megfelelően védjék a bennük tárolt (pl. konfigurációs vagy naplózási) adatokat is.	△ Nem nevesíti konkrétan a szenzorokat, de minden hálózatra kapcsolt és digitális komponensre vonatkozik, tehát ide értendő.	✗ Nem vonatkozik közvetlenül a járművek belső buszprotokolljaira, mivel azok nem „általános digitális termékek” (nem kaphatók külön a piacon). A belső járműprotokollokat (pl. CAN) csak akkor érinti, ha azok önállóan is digitális terméknek minősülnek, ami a gyakorlatban ritka.	✓ Kifejezetten szabályozza a beágyazott szoftver (firmware) biztonságos fejlesztését, frissítését és támogatását.	△ Előírja a beszállítói lánc transzparenciáját, a komponensek biztonságát, és kötelezővé teszi a biztonsági események bejelentését is. Közvetlen felelősség, ha önállóan piacra lép az EU-ban; közvetett felelősség, ha OEM-hez szállít A gyártó auditálhatja vagy visszautasíthatja a beszállítói komponenst.	✗ Nem célja a felhasználói védelem.	**11**	**Közepes erejű**
GDPR	Kötelező	Pénzbírságok (akár a globális éves forgalom 4%-áig)	EU tagállami adatvédelmi hatóságok	△ Csak akkor érinti, ha hozzáférés személyes adathoz történik.	△ Adatkezelés, jogalap, biztonsági elvárások, de nem minden adattípust vizsgál.	✗ Nem technikai szintű. Csak ha személyes adat.	✗ Nem vonatkozik rá.	✗ Nem kezeli.	△ Közös adatkezelés esetén szabályozza a felelősséget és csak adatvédelmi szempontból.	✓ Kifejezetten ezek védelme a cél. Kötelező.	**8**	**Alacsony erejű**
CISPR 25	Általában kötelező	Forgalmazási engedély megtagadása	Nemzeti hatóságok	✗ Csak EMC-vel foglalkozik.	✗ Csak EMC-vel foglalkozik.	✗ Csak EMC-vel foglalkozik.	✗ Csak EMC-vel foglalkozik.	✗ Csak EMC-vel foglalkozik.	✗ Csak EMC-vel foglalkozik.	✗ Csak EMC-vel foglalkozik.	**3**	**Nem megfelelő**
TISAX	Nem kötelező	Szerződéses kizárás lehetséges	ENX Association	✗ Nem foglalkozik vele.	✓ Auditálási keret az adatbiztonságra – de nem technikai védelem. Vállalati szintű.	✗ Nem foglalkozik vele.	✗ Nem foglalkozik vele.	✗ Nem foglalkozik vele.	△ Auditálási keret az adatok biztonságára – de nem technikai védelem. Vállalati szintű.	✓Figyelembe veszi.	**6**	**Alacsony erejű**

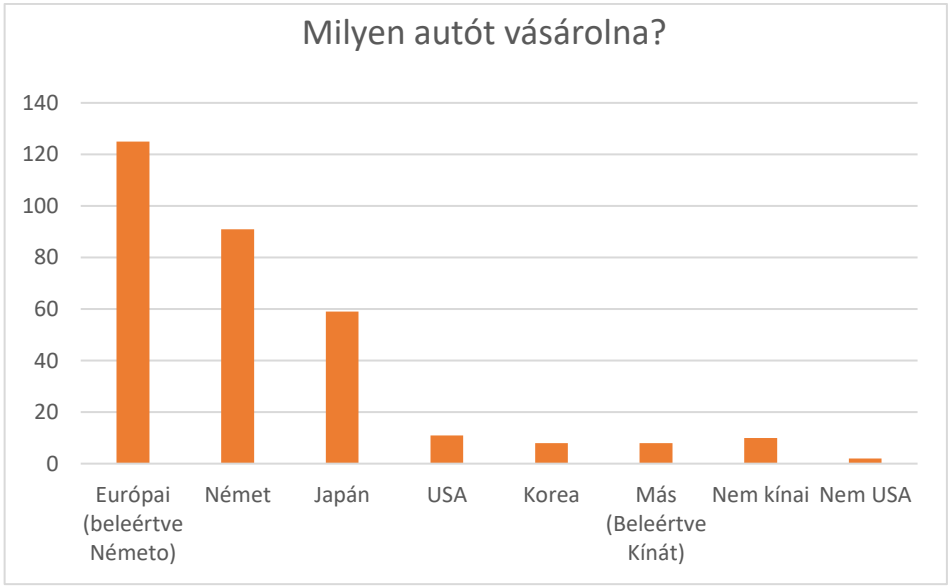
Szabályozás	Kötelező	Szankció	Felügyelet	Távoli elérés	Tárolt adatok	Szenzor	CAN	Firmware	Beszállítói lánc	Személyes adatok	Pont	Besorolás
SAE J3061	Nem kötelező	Nincsenek jogi szankciók, de reputációs hátrány, piacvesztés lehet	Nincs hivatalos felügyelet	✓ Elfogadott gyakorlatokat ír elő, de nem kötelező. Nincs hatósági ellenőrzés.	△ Emlegeti, de részletesen nem szabályozza.	△ Emlegeti, de részletesen nem szabályozza.	△ Emlegeti, de részletesen nem szabályozza.	✓ Elfogadott gyakorlatokat ír elő, de nem kötelező. Nincs hatósági ellenőrzés.	△ Elfogadott gyakorlatokat ír elő.	△ Részletesen nem szabályozza, utal rá.	**9**	**Közepes erejű**
ASPICE	Nem kötelező	OEM kizárhatja a beszállítót	Autógyártói audit	△ Technológiai alapot nyújt, de nem szabályozza a védelmi megoldást.	✗ Nem tárgyalja ezt a területet.	✗ Nem tárgyalja ezt a területet.	✗ Nem tárgyalja ezt a területet.	✓ Architektúra és fejlesztési folyamat szintjén támogatja a biztonságos implementációt.	✓ Architektúra és fejlesztési folyamat szintjén támogatja a biztonságos implementációt.	✗ Nem tárgyalja ezt a területet.	**5**	**Alacsony erejű**
ISO 21448	Nem kötelező	Nincsenek közvetlen szankciók	Nincs hivatalos felügyelet	✗ Nem célja ehhez hasonló fenyegetések kezelése.	✗ Nem célja ehhez hasonló fenyegetések kezelése.	✓ A tervezett funkcionalitás hibáinak elemzése során szenzorok hibáira fókuszál. Funkcionális szempontból részletes.	✗ Nem célja ehhez hasonló fenyegetések kezelése.	✗ Nem célja ehhez hasonló fenyegetések kezelése.	✗ Nem célja ehhez hasonló fenyegetések kezelése.	✗ Nem célja ehhez hasonló fenyegetések kezelése.	**1**	**Nem megfelelő**
NHTSA Cybersecurity Guidelines	Nem kötelező	Nincsenek hivatalos szankciók, reputációs kockázat lehetséges	NHTSA (USA)	△ Erős ajánlásokat tartalmaz, de nem jogilag kötelező. Amerikai gyártóknak ajánlott követni.	✗ Érinti, de nem szabályozza kötelezően.	✗ Érinti, de nem szabályozza kötelezően.	△ Erős ajánlásokat tartalmaz, de nem jogilag kötelező. Amerikai gyártóknak ajánlott követni.	△ Erős ajánlásokat tartalmaz, de nem jogilag kötelező. Amerikai gyártóknak ajánlott követni.	△ Erős ajánlásokat tartalmaz, de nem jogilag kötelező. Amerikai gyártóknak ajánlott követni.	△ Érinti, de nem szabályozza kötelezően.	**6**	**Alacsony erejű**

22. táblázat - Szabványok és jogszabályok összehasonlító elemzése megfelelőségi és védelmi szempontok alapján. Forrás: saját forrás

7. Számú melléklet – Empirikus kutatási eredményekhez kapcsolódó ábragyűjtemény

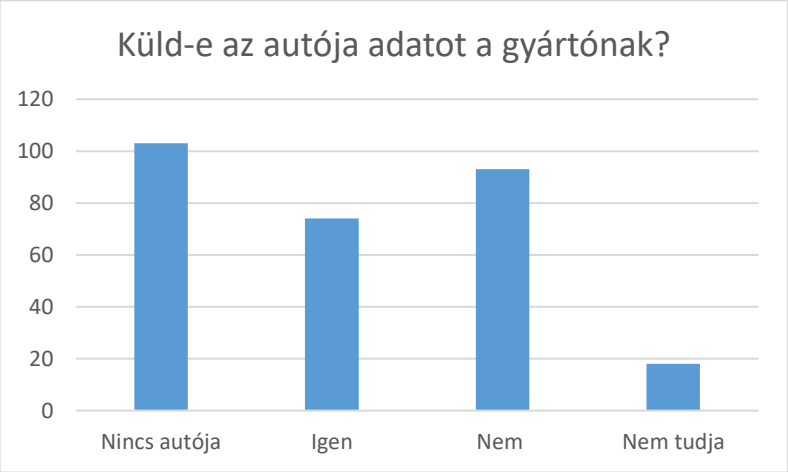


13. ábra - A válaszadók definíciójában leggyakrabban előforduló gondolati koncepciók. Forrás: saját forrás.

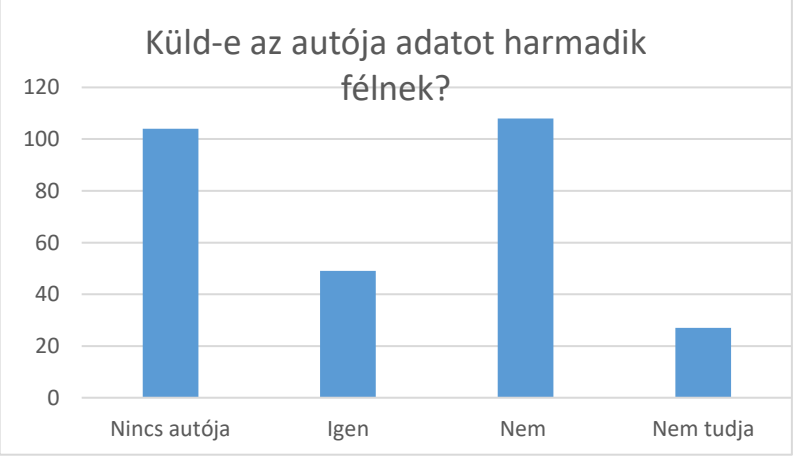


14. ábra - Országpreferenciák származási országok bontásában. Forrás: saját forrás.

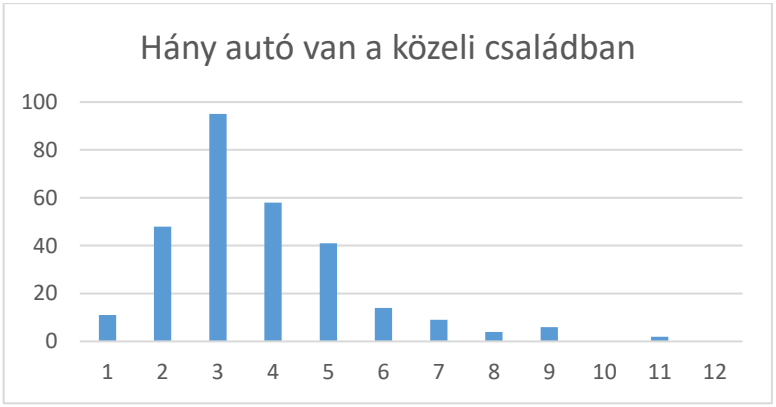
15. ábra - A nem preferált származási országokkal kapcsolatos ellenérzések természete kategóriákra bontva. Forrás: saját forrás.



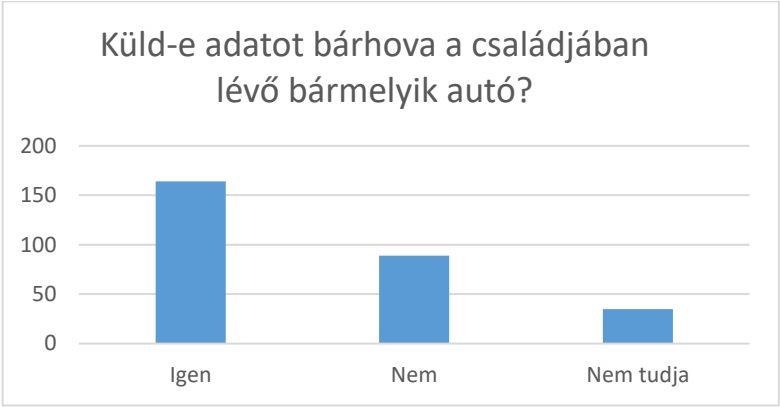
16. ábra - Kérdőíves kérdés a személygépjármű által küldött adatokra vonatkozóan (gyártó). Forrás: saját forrás.



17. ábra - Kérdőíves kérdés a személygépjármű által küldött adatokra vonatkozóan (harmadik fél). Forrás: saját forrás.



18. ábra - A kérdőív válaszadóinak családjának tulajdonában lévő személyautók száma. Forrás: saját forrás.



19. ábra - A család tulajdonában lévő személyautók adatküldésére vonatkozó gondolatok. Forrás: saját forrás.

8. Számú melléklet – A kérdőíves kutatás során gyűjtött adatok ellenőrzése

A kérdőíves kutatás során gyűjtött adatok megbízhatósága kulcsfontosságú kérdés, mivel ezek képezik az alapját annak az elemzésnek, amely az internetkapcsolattal rendelkező személygépjárművek elfogadottságát, valamint az ezekhez kapcsolódó adatvédelmi kockázatok ismertségét vizsgálja. A kérdőív jelentős részét nyílt végű kérdések alkották, amelyek lehetővé tették a válaszadók egyéni nézőpontjainak feltérképezését. Az ilyen válaszok minősége és tartalma már önmagukban is fontos indikátorai lehetnek a válaszadók komolyságának és tájékozottságának.

A kvalitatív megbízhatóságot az biztosítja, hogy a válaszadók válaszai egyértelműen tükrözik az elmélyült gondolkodást és az őszinte véleményformálást. Például egy válaszadó az alábbi módon fogalmazta meg az „okosautó” definícióját: „*Self-driving capabilities at a human level of driving—not just stopping abruptly when there's an*

obstacle or crashing into a wall, but actually navigating from point A to point B. I suppose a smart fridge doesn't need nearly as much to be considered 'smart.'"(azaz „Önvezető képességek emberi szintű vezetési teljesítménnyel – nem csupán annyi, hogy hirtelen megáll, ha akadály van előtte, vagy nekimegy a falnak, hanem valóban képes eljutni A pontból B pontba. Feltételezem, hogy egy okoshűtőnek ennél jóval kevesebb is elég ahhoz, hogy 'okosnak' nevezzük.") Az ilyen részletes válaszok alapján megbízható következtetések vonhatók le. Az adattisztítás során kizárásra kerültek azok az esetek (összesen három), amelyeknél felmerült a nem őszinte válaszadás gyanúja.

Tovább növeli az adatok hitelességét, hogy a kérdőív kitöltése semmilyen módon nem volt jutalmazva, azaz nem kapcsolódott hozzá sem sorsolás, sem egyéb érdekeltség. A válaszadás teljes mértékben önkéntes alapon történt. A válaszok numerikus validálását is elvégeztem. A szöveges válaszokat először kulcsszavak alapján számszerűsítettem (0 – nem szerepel, 1 – szerepel), például az „okosautó" definícióját vizsgáló kérdés esetén a következő szempontok szerint: internet, szoftver, IoT, fejlett vezetési funkciók, elektromos hajtás, adatátvitel, szenzorok, önvezetés, mobilalkalmazás. Ehhez első lépésben a szöveges válaszokat numerikus adattá kellett konvertálnom, amelyet az alábbi módon tettem meg: A kifejtős kérdésekben kulcsszavak meglétét kerestem mint pl. "A mit ért okosautó alatt" kérdésnél (15. táblázat): A: Internet, B: Software, C: IoT, D: Advanced driving functions, E: Electric car, F: Data transfer, G: Sensors, H: Self-driving, I: mobile app. Az így nyert bináris mátrix jól használható volt további megbízhatósági vizsgálatokhoz:

	A	B	C	D	E	F	G	H	I
	Internet	Software	IoT	Advanced driving functions	Electric car	Data transfer	Sensors	Self-driving	Mobile app
	Internet	Szoftver	IoT	Fejlett vezetési funkciók	Elektromos autó	Adat-továbbítás	Szenzorok	Önjáró/ autonóm	Mobilalkalmazás
0	1	0	0	0	0	0	0	0	1
1	0	0	0	1	0	0	0	1	0
2	0	0	0	1	0	0	1	1	0
…									
n									

23. *táblázat - Kulcsszó-alapú bináris kódolás az okosautó fogalmának felhasználói értelmezésére (minta), a teljes számítás a következő GitHub repositoryn érhető el: https://github.com/hhenrietta/smarcar_survey . Forrás: saját forrás.*

9. Számú melléklet – Poisson-folyamat

A Poisson-folyamat **képlete**:

$$P(k) = \frac{\left(\lambda^k \, e^{\{-\lambda\}}\right)}{k!}$$

ahol

- N: az időegység (pl. perc) alatt elhaladó események (autók) száma,
- k: a keresett esetszám (pl. hány autó halad el az objektum előtt),
- λ: az időegységre jutó átlagos elhaladás (pl. percenként 10 autó).

A várható érték (E[N]) pedig:

$$E[N]=\lambda$$

Azaz, ha egy sávban percenként átlagosan 10 autó halad el, akkor λ = 10.
A *kompromittált* autók esetén azzal számolunk, hogy a támadó a teljes forgalom egy adott hányadát (p) tudja megfigyelésre használni, így a várható szám:

$$E[N_{komp}]=\lambda \cdot p$$

Példa:
Ha λ = 20 autó/perc, és a támadónak a városi forgalom 0,5%-át kitevő 1000 autót sikerül kompromittálnia a teljes 200 000 autóból, akkor:

$$p = \frac{1000}{200000}$$

$$E[N_{komp}]=20 \cdot 0{,}005=0{,}1$$

(várhatóan minden 10. percben halad el egy kompromittált autó)

10. Számú melléklet – Problémakörök és megoldási javaslatok

Fő probléma	Gyakorlati megoldás – javaslat
Szabályzati töredezettség, hatósági átfedések	Egységes kockázatmenedzsment-kézikönyv és eljárásrend minden piaci szereplőnek; központi hatósági „kapu” kialakítása, amely minden jogszabályi megfelelésre (NIS2, GDPR, CRA, UNECE R155/R156 stb.) integrált útmutatót és kapcsolatfelvételi lehetőséget nyújt.
Felhasználók tájékoztatásának hiánya, átláthatatlanság	Nyilvános, többnyelvű, online információs portál a járműipari kiberbiztonságról és fogyasztói jogokról; rendszeres hatósági tájékoztatók, esettanulmányok, ajánlott védelmi gyakorlatok; gyors, érthető incidens-jelentési lehetőség a végfelhasználók részére.
Egységes kockázatelemzési megoldás hiánya	Minden szereplőre kiterjedő, auditálható, minimumkövetelményeket tartalmazó kockázatelemzési keretrendszer (pl. kötelező TARA-adaptáció szervezeti szintre, kockázati indikátor lista az auditokhoz); a hatóság ellenőrizze, hogy a valós, nem formális (nem csak tankönyvi) fenyegetések is szerepelnek-e az elemzésekben; gyakorlati példatár és folyamatos, központi visszacsatolás, mit értékeltek alul az auditok során.
Műszaki problémák (titkosítás hiánya/gyengesége, protokollhibák)	Protokoll-lista publikálása, amely felsorolja, hogy az egyes autóipari adatkapcsolati rétegek milyen biztonsági szintet teljesítenek (pl. van-e titkosítás, hitelesítés); „hiányos” protokolloknál kötelező frissítési, javítási, vagy mitigációs terv benyújtása a hatóság felé; összehasonlító audit, amely a különböző OEM-ek és beszállítók technikai védelmi szintjeit is összeveti.
Rejtett, állami vagy privilegizált szereplő által kihasználható fenyegetések (covert channel)	A kockázatmenedzsmentnek kötelezően ki kell térnie a nem-konvencionális (pl. állami, belső vagy beszállítói) fenyegetési vektorokra is; audit során a rendszeresített jelentési kötelezettség minden ilyen esetre, közvetlenül az EU-szintű hatósághoz; részletes threat modeling szcenáriók, amelyek feltárják, hogy milyen adatmozgások használhatók illegális vagy nem-eredeti célú adatáramlásra; központi támogatás (mintaszkriptek, modellezési guideline-ok), hogy a szervezetek ilyen fenyegetéseket is be tudjanak építeni a saját elemzéseikbe.
Átláthatóság, visszacsatolás, közös szakmai minimum	Centralizált, anonim audit- és kockázatelemzési adatbázis, amelyhez minden szereplő (OEM, beszállító, hatóság, auditcég) jelenthet, és amelyből esettanulmányok, tipikus hiányosságok, sikeres megoldások elérhetők – folyamatos tanulási platformként szolgálva.

24. táblázat - Javasolt gyakorlati megoldások, melyeket a leendő hatóságnak alkalmaznia kell. Forrás: saját forrás

13. FŐBB JOGSZABÁLYOK, SZABVÁNYOK, SZABÁLYOZÁSOK

Forrás neve	Elérési út / link
ISO/SAE 21434 – Road Vehicles Cybersecurity Engineering	https://www.iso.org/standard/70918.html
UNECE WP.29 – R155 & R156	https://unece.org/transport/vehicle-regulations/wp29/new-vehicle-regulations
Cyber Resilience Act (CRA)	https://eur-lex.europa.eu/legal-content/HU/TXT/?uri=CELEX:32024R1805
ISO 26262 – Functional Safety for Road Vehicles	https://www.iso.org/standard/68383.html
GDPR – General Data Protection Regulation (EU 2016/679)	https://eur-lex.europa.eu/eli/reg/2016/679/oj
NIS2 – Network and Information Security Directive (EU 2022/2555)	https://eur-lex.europa.eu/eli/dir/2022/2555/oj
TISAX – Trusted Information Security Assessment Exchange	https://enx.com/tisax/
ISO/IEC 27001 – Information Security Management	https://www.iso.org/isoiec-27001-information-security.html
ISO/IEC 15408 – Common Criteria	https://www.commoncriteriaportal.org/
AUTOSAR Adaptive Platform	https://www.autosar.org/standards/adaptive-platform/
ASPICE – Automotive SPICE	https://www.automotivespice.com/
NIST Cybersecurity Framework	https://www.nist.gov/cyberframework
NHTSA Cybersecurity Best Practices	https://www.nhtsa.gov/technology-innovation/vehicle-cybersecurity
ISO 21448 – Safety of the Intended Functionality (SOTIF)	https://www.iso.org/standard/70939.html
ISO 24089 – Software Update Engineering	https://www.iso.org/standard/75177.html
CISPR 25 – Vehicle EMC	https://webstore.iec.ch/publication/6364

25. táblázat – Főbb jogszabályok.. Forrás: saját forrás

14. 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

26. táblázat – Rövidítések jegyzéke. Forrás: saját forrás

15. ÁBRAJEGYZÉK

16. TÁBLÁZATJEGYZÉK