

37. Országos Tudományos Diákköri Konferencia
Had- és Rendészettudományi Szekció
Budapest, 2025. április 22-24.
Nemzeti Közsolgálati Egyetem
Hadtudományi és Honvédtisztképző Kar

**Digitális kulcs a bűnelkövetők
kezésében: a gépjárműlopás új
módszerei és büntetőjogi megítélésük**

Jelige: Kibertér

Pályamunka lezárásának időpontja: 2024. december

2025.

Tartalom

1. Bevezetés	2
2. Az új „okosautók” feltörése	5
2.1. A technikai fejlődés	5
2.2. Az immobiliser	7
2.3. Relay-támadás	8
3. Lopásgátló eszközök	12
3.1. Fizikai akadályok	12
3.2. Nem fizikai akadályok	13
4. Tesla	14
4.1. A Tesla járművek lehetséges nyitási módjai	14
4.2. A Tesla autók védelme	15
4.3. Etikushacker-verseny, ahol mindenki nyer	17
5. Lopás vs. az információs rendszer vagy adat megsértésének bűncselekménye	18
5.1. Lopás	18
5.2. Információs rendszer vagy adat megsértése	21
5.3. A bűncselekmény minősítésének dogmatikai kérdései	23
6. Következtetések	25
7. Irodalomjegyzék	28

1. Bevezetés

Az első autó megjelenésétől fogva sejteni lehetett, hogy ezek a járművek az ember életében meghatározó szerepet fog játszani. Kezdetben elsősorban, mint használati tárgyként, később pedig mint kényelem és az életminőség javításának funkciójaként terjedtek el. Az évek múlásával ez az állapot csupán erősödött olyannyira, hogy mára a társadalomban betöltött szerepük kibővült, a mindennapi életünk részévé vált. Azonban érdemes kiemelni, hogy még mindig egyfajta luxuscikknek számít, hiszen egyrészt nem minden ember engedheti meg magának, hogy rendelkezésére álljon legalább számára egy autó, hiszen annak beszerzése és fenntartása komoly anyagi áldozatokat követel. Másrészt nagyban növeli a kényelmi érzetet, amelyet sokan a luxus egyik alapvető mércéjének tekintenek. Munkába járásnál, mindennapi ügyeink elintézésében, kikapcsolódás vagy utazás esetén jelentős szerepet tölt be.

A kényelem egy nagyon vonzó, egyben veszélyes dolog. Ahogyan azt tapasztaljuk életünk során szinte minden jó dolognak megvan a rossz, számunkra hátrányos oldala is. Nincs ez másképpen az gépjárművek esetében sem. A kényelmi elvárások kielégítésére a napjainkban megjelenő autók rengetek technikai eszközzel vannak felszerelve, gondolok itt a beépített érintőképernyős kijelzőre, sávtartó és ütközésselkerülő rendszerre stb. Mindezek működéséért, valamint a védelmi rendszer üzemeltetéséért a gépjárművekbe beépített információs rendszer felel. Ez a fő mozgatórugó, a legfontosabb és egyben legsebezhetőbb része az autóknak, amely a bűnözők érdeklődését is felkeltette.

A technika fejlődésével nem csupán az élet kényelmesebbé tételére irányuló eszközök váltak egyre kifinomultabbá, hanem a bűncselekmények elkövetési magatartásai, módjai is megváltoztak. Az autólopások területén különösen szembetűnő ez a tendencia. Jellemzővé vált, hogy az elkövetők ma már gyakran nem mechanikai eszközökkel vagy erőszakkal próbálnak meg behatolni egy gépjárműbe, hanem annak védelmi rendszerét játszák ki és ennek segítségével tulajdonítják el azt. Azonban nem egyértelmű, hogy ebben az esetben milyen bűncselekmény valósul meg pontosan, hiszen egyrészt felmerül a dolog elleni erőszakkal elkövetett lopás, másrészt viszont – emellett vagy ezzel párhuzamosan – az információs rendszer vagy adat megsértésének vétsége.

A téma körül-járásával célom, hogy bemutassam milyen veszélyek fenyegetnek minket, illetve az új, ún. „kulcsnélküli” autók a modern világban, valamint, hogyan lehet ellenük a leghatékonyabban védekezni. Mindemellett részletesen vizsgálom a fentebb említett két bűncselekményt abból a szempontból, hogy melyik deliktum megállapításának lenne helye a modern autólopás kapcsán, esetleg felmerülnek-e a heterogén alaki halmazokban állásuk

feltételei. A fő és egyben kiinduló kérdés pedig: miért fordul elő egyre többször a tárgyalóteremben, hogy a bíróság és az ügyészség eltérő álláspontot képvisel ezekben az ügyekben?

2. Az új „okosautók” feltörése

„Okosautónak” nevezhetjük a továbbiakban azokat a gépjárműveket, amelyek fejlett elektronikai berendezésekkel rendelkeznek, valamint a működésükhöz informatikai rendszerre van szükség.

2.1. A technikai fejlődés

Régen nem jelentette vita tárgyát milyen bűncselekmény valósult meg egy autólopás esetén. Az elkövetők manuálisan nyitották fel a zárat, húzták le az ablakokat, mindezt úgy, hogy az esetek többségében társult hozzá a gépjárműben bekövetkezett állagsérelem is. Ezt hívjuk dolog elleni erőszakkal elkövetett lopásnak.

Az autólopás technikái az évek során folyamatosan fejlődtek, párhuzamosan az autók technológiai fejlődésével. Ahogy a gyártók újabb biztonsági rendszereket fejlesztenek ki, a tolvajok is egyre kifinomultabb módszerekkel próbálják meg kijátszani ezeket. Íme egy áttekintés az autólopás technikai fejlődéséről:

Az elkövetőket két dolog vezérelheti autólopás esetén: az egyik lehetséges indok a kényelmi ok, amely jelentheti azt, hogy saját felhasználás tulajdonítják el a gépjárműveket vagy más bűncselekmények elkövetéséhez szolgálhat eszközül.¹ A másik, egyben nagyobb hasznot hozó magyarázat az üzletszerűen végzett illegális autókereskedelem.² Számos olyan bűnszervezet létezik, akik tolvajokat bíznak meg kiszemelt autók ellopása érdekében.

A hagyományos, mondhatni régmódon nyíló gépjárműveket, a tolvajok kreativitására bízva, többféleképpen is ki lehet nyitni. Az elkövetés módszere változó, akár tolvajonként különböző lehet, vagyis az ellopni kívánt autó (célautó) kiválasztása, annak eltulajdonítása, valamint az autótól való megszabadulás módja szintén változó. Az egyik legelterjedt eszköz az ún. Turbodecoder, amely egy kisebb méretű, viszont annál hasznosabb és gyorsabb szerkezet.³ Segítségével akár 10-15 másodperc alatt nyitódnak a záruk, és, mivel képes rögzíteni a szükséges kódot, ezért a továbbiakban a kormányzár kiiktatásával sem lesz már problémája az elkövetőnek.⁴ Ezt követően a tolvajnak egyetlen feladata maradt: hatástalanítsa az indításgátlót, amelyhez pusztán egy diagnosztikai csatlakozóra van szüksége.⁵ Ezenkívül bevált módszer

¹ MIKEL Longman: The problem of auto theft, In: Forensic Investigation of Stolen-Recovered and Other Crime-Related Vehicles, pp.2., 2016

² u.o.

³ SZAYER Géza – KOVÁCS Bence: Gépjárművédelmi megoldások a modern lopási módszerek ellen, Recent Innovations in Mechatronics 6: 1 pp. 1-6., 6.p., 2019

⁴ u.o.

⁵ u.o.

bármilyen olyan eszköz, amivel fel lehet feszíteni az ajtót, ablakot, illetve bizonyos módszerrel a ragasztószalag is alkalmas lehet az autóba való bejutásra.

Napjainkban a gyárakból kigördülő autók többségét olyan technikai berendezésekkel látják el, mint a beépített navigáció, wifi vagy Bluetooth-os csatlakozás lehetősége. A működésükhöz azonban elengedhetetlen bizonyos hardverek és szoftverek megléte. Némi túlzással azt lehet mondani, hogy „kerekeken guruló adatközpontokká” váltak.⁶ Az internethez csatlakoztatott autók folyamatosan feldolgozzák a bejövő és kimenő adatokat.⁷ Az ilyen intelligens technológia egy kétirányú, vezeték nélküli kapcsolatra támaszkodik, amelynek a legnagyobb hátránya, hogy feltörhetőbbé teszi a járművet.⁸ A kétirányú kommunikáció a jármű és a kártya között jön létre.⁹ Abban az esetben, ha a kártya valamilyen oknál fogva nem tudja venni az autó jelét, a gépjármű indítása elektronikusan le lesz tiltva.¹⁰ Ez azt jelenti, hogy az autó nem fog elindulni, vagy, ha a motor már jár, azonban a kulcs hirtelen kikerül az utastérből, nem fog megmozdulni. Az autólopás elkövetőjének egyik célja, hogy a jármű és a kártya között fennálló kapcsolatot és jeleken keresztül való kommunikációt befolyásolja, így felvetődik a kérdés: hogyan lehet megkülönböztetni a tolvaj által generált jelet az eredetitől?¹¹ Ezért is fontos a megfelelő biztonsági védelem. Minden új szolgáltatás és képesség új belépési pontokat teremt, amely csak növeli az adatszivárgás lehetőségét.¹²

Az utóbbi időben tehát megnőtt azoknak a járműveknek a száma, amelyek működésében és védelmében fontos szerepet játszik az információs rendszer, kiszélesítve ezáltal a bűnözők mozgásterét. A támadó technikák folyamatosan fejlődnek és egyre több eszköz áll a rendelkezésükre is. Ez jelenti az egyik fő problémát: ezek az eszközök és kellékek beszerzése nem okoz akadályt az elkövetők számára, mivelhogy az internet segítségével könnyedén hozzá tudnak jutni bizonyos internetes oldalakon keresztül, akár olyan ismert webhelyen is, mint például az Amazon vagy az eBay, nem mellesleg megfizethető áron.

A másik legfőbb probléma, hogy az autógyárak a lehető legrövidebb idő alatt szeretnék piacra juttatni a járműveket, így nem fordítanak elegendő időt a megfelelő biztonsági rendszer beépítésére. Egy hatékonyabb védelmi rendszer kiépítése bizony időigényes, akár évekbe is

⁶ JAMES Hayes: Hackers under the hood: It's been five years since the first reports of car hacking emerged, but despite progress in vehicle protection standards, automotive cyber-security remains on high alert, E&T Magazine, Volume 15, Issue 03, 2020, page 32.

⁷ u.o.

⁸ u.o.

⁹ LADVÁNSZKY János: Az autólopás elleni védekezés egy lehetséges módszere (kulcs nélküli indítórendszeres gépkocsik esetén), In: *Híradástechnika*, 57. Évfolyam, 2002/5. sz., 55. o.

¹⁰ u.o.

¹¹ u.o.

¹² JAMES Hayes: Hackers under the..., page 32.

telhet. Azonban az autók ellen irányuló kiberfenyegetések veszélye igen is napról napra nő. Egyes források szerint csupán 2018 és 2019 között megkétszereződött a kiberbiztonsági incidensek száma.¹³ Fontosnak tartom a probléma minél előbbi megoldását, hiszen egyrészt több millió értékű károkat okozhatnak a bűnözők, másrészt akár az emberi életek is veszélybe kerülnének, ha bárki átvenné az irányítást egy jármű felett.

2.2. Az immobiliser

Az indításgátló, vagy más néven immobiliser, a gépjárműbe gyárilag beépített biztonsági rendszer, melynek fő feladata, hogy jelezzen, ha jogtalan indítási kérést észlel.¹⁴ Egy kommunikációs csatorna jön létre a kulcs által tartalmazott integrált áramkör (transponder) és a motorvezérlő között.¹⁵

Működésének alapja egy számítástechnikai rendszer, amelyet ECU-nak (Engine Computer Unitnak) nevezünk. A motor elindítása esetén az ECU lekérdezi az immobilizertől a beérkező kódot, majd azt összeveti, valamint leellenőrzi a kulcs és a rendszer között fennálló algoritmus segítségével.¹⁶ Az azonosítás sikeres megtörténte után a gyújtáskapcsoló egy jelet küld a motorvezérlő indításgátló moduljához, és azonos kód esetén engedélyt ad a gyújtásra.¹⁷ Abban az esetben viszont, ha eltérést érzékel a rendszer az eltárolt kód és a transponder által küldött kód között, nem ad engedélyt a motor indítására.¹⁸

Utólag is van rá lehetőség, hogy beszereljük. Ezek általában nagyobb védelmet biztosítanak, kevésbé kizárhatóak, mivel egyedileg meghatározottak és nem pedig tömegesen helyezik be őket a gyártósoron gördült autókba.¹⁹ Olyan elektronikus rendszer, amely egyben három pont letiltására is alkalmas: az önindítót, a gyújtást és az üzemanyagot is képes blokkolni. Bármelyik hiánya esetén az autó motorja nem indítható el.²⁰ Ennek feloldása többféleképpen történhet, például kód beírásával vagy egy kulcs meghatározott helyhez történő érintésével.²¹

Szükséges kiemelnem, hogy az indításgátló működésébe történő jogosulatlan beavatkozás csak akkor lehetséges, ha az elkövető célja a gépjármű elvétele. Mindemellett

¹³ u.o.

¹⁴ Zs+u honlapja, Indításgátlók, In: https://zsu.hu/autoelektronika-inditasgatllok?srsId=AfmBOoqVru8IRTjX21bdra8Pij4sxnWVlJQj8L1SDXMEzM_DOZvvcWtH (Megtekintve: 2024.10.31.)

¹⁵ u.o.

¹⁶ u.o.

¹⁷ u.o.

¹⁸ u.o.

¹⁹ u.o.

²⁰ As Solutions honlapja, In: <https://assolutions.hu/blog/164/gepjarmuvedelmi-kisokos-mi-az-immobiliser-es-az-auto-lopasgatllo> (Megtekintve: 2024.10.17.)

²¹ u.o.

megállapítható, hogy az immobiliser fogalma beletartozik a Btk. által meghatározott információs rendszer²² definíciójába.

2.3. Relay-támadás

Manapság a legtöbb új autó már a hozzá tartozó kulcs fizikai használata nélkül kinyitható. Elegendő, ha a jármű közelében van a kulcs, akár a táskánkban vagy a zsebünkben. Egy laza kézmozdulat az ajtónál, és már nyílik is a zár. Ehhez igazodva az autótolvajoknak is változtatniuk kellett az elkövetési módszereiken, hogyan tudják eltulajdonítani az általuk kiszemelt járművet. Azonban, mint tudjuk számukra sosem jelent gondot az alkalmazkodás.

Az ilyenfajta gépjárművekkel szemben többféle, ún. kulcsnélküli támadás hajtható végre:

- Remote Keyless Entry (Relay Attack),
- Replay Attacks,
- Roll Jam Attacks,
- Roll Back Attacks,
- CAN Injection Attacks.²³

A bűnözők körében elterjedt az úgynevezett jelfogó támadás (*relay attack*, a továbbiakban relay-támadás), egy újfajta digitális lopási technika, amellyel a kulcs nélkül beléptető és indító rendszerek sebezhetőségét használják ki. Tulajdonképpen minden kulcs nélkül nyitható és indítható gépjármű ki van téve ennek a veszélynek. A tolvajok kifinomult technológia segítségével képesek behatolni és feltörni az autó számítógépes rendszerét és ennek következtében átvenni az irányítást. Ezalatt azt értem, hogy fel tudják oldani a zárat, valamint a kulcs hozzájárulása nélkül be tudják indítani a járművet és végül könnyedén elhajthatnak.

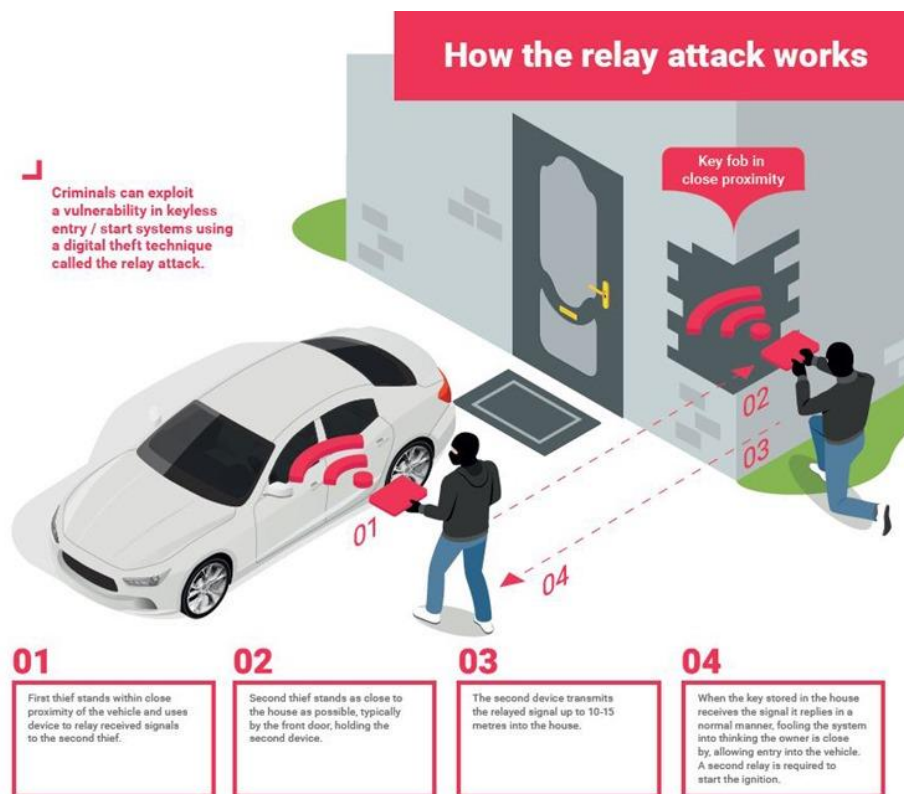
Hogyan hajtják végre a támadást? Általában két ember összehangolt tevékenységére van szükség. Ahogyan az 1.ábra is mutatja, az egyikük a célba vett jármű mellett áll, a másik pedig a lehető legközelebb ahhoz a házhoz, amelyben a kulcs, illetve a kulcsként szolgáló telefon található.²⁴ Mindkettő személynek rendelkeznie kell egy bizonyos készülékkel, amely könnyen beszerezhető. Ugyan az esetek többségében az elkövetők lakott területen belül csapnak le, olyan helyeken, ahol viszonylag közel parkolnak az autók a házhoz, egyes eszközök hatótávolsága

²² A Btk. 459. § (1) bekezdésének 15. pontja értelmében: információs rendszer az adatok automatikus feldolgozását, kezelését, tárolását, továbbítását biztosító rendelkezés, vagy a biztosító berendezés, vagy az egymással kapcsolatban lévő ilyen berendezések összessége.

²³ NAIR, VINAY Unnikrishnan: Smart car hacking: a threat to the rising automotive industry, In: <https://esource.dbs.ie/server/api/core/bitstreams/e87a1b88-c877-458a-a5ca-867fb09f51de/content> (Megtekintve: 2024.10.07.)

²⁴ Keyless car theft: What is a relay attack, how can you prevent it, and will your car insurance cover it?, In: <https://leasing.com/guides/relay-car-theft-what-is-it-and-how-can-you-avoid-it/> (Megtekintve: 2024.10.06.)

elérheti a 100 métert is²⁵, megkönnyítve ezzel a bűnözők dolgát. Első lépésben az autó közvetlen közelében álló tolvaj (a továbbiakban egyes számú tolvaj) a kezében lévő készülék segítségével kulcsnak adja ki magát és jelet küld a jármű rendszerének. A rendszer érzékeli a bejövő jelet, azonban megkéri a kulcsot, hogy hitelesítse magát.



1. ábra: Hogyan működik a relay-támadás?²⁶

Mivel az egyes számú tolvaj ezt nem tudja megtenni, ezért második lépésként ezt a „kérést” tovább küldi az eszközön keresztül a kettes számú tolvajnak, aki a ház mellett tartózkodik. Harmadik lépésben a második elkövető, a nála lévő készülékkel, elküldi a jelet a fal másik oldalán található kulcsnak, amely válaszként visszaküldi az autó ajtajának nyitásához szükséges hitelesítő adatokat. Figyelniük kell az elkövetőknek, hogy mivel az eszköz hatósugara körülbelül 10-15 méter, ezért a kulcsnak ezen a távolságon belül kell lennie, különben nem járnak sikerrel.

²⁵ u.o.

²⁶ u.o.

Végül, a megszerzett adatokat a kettes számú tolvaj megküldi az egyes számú tolvajnak, aki egyből továbbítja is azokat a jármű felé, megtévesztve ezzel a rendszert. Elhíttetik vele, hogy a tulajdonos a közelben van a kulccsal, vagy bizonyos esetekben a telefonnal együtt, és ezért kinyitódhatnak az ajtók.

Ahhoz, hogy a jármű el is induljon, egy második körös támadásra is szükség van.²⁷ Az autó rendszere érzékeli, hogy az ajtók nyitva vannak már, viszont újból megkérdezi, hogy elérhető-e a kulcs. Tehát miután az első tolvaj bejutott a kocsiba meg kell ismételni a folyamatot. El kell küldenie a másik tolvajnak a kérést, ő pedig küldi a kulcstól érkező adatokat válaszként, és a jármű indulásra készen.

Ez a helyzet megvalósulhat a legváratlanabb pillanatokban, akár egy kávézóban is, ahol az egyik elkövető mögöttünk áll, míg a másik kint várja a jelet a jármű mellett. Nem telik el egy perc és a tulajdonunk máris veszélybe kerül. Az olcsó és viszonylag egyszerű technika több száz jármű ellopására alkalmas, márkától függetlenül.

Hogyan lehet védekezni ellene? A következőkben felsorolásra kerül néhány hasznos javaslat a relay-támadás, valamint a közönséges járműlopások elkerülése érdekében:

- **Blokkoljuk valamilyen módon az elektronikus kulcs jeleit.** Léteznek úgynevezett Faraday-stílusú tárcák, kulcstartók, amelyek rendkívül hatékony módon blokkolják az elektronikus jeleket, így nem férhet hozzá illetéktelen személy. Ha egyszerűbb megoldást szeretnénk szimplán rakjuk az elektronikus kulcsunkat a hűtőszekrény mellé, esetleg tegyük egy fémdobozba vagy az alá, hiszen a fém blokkolhatja a jelet, ezzel védelmet biztosít az esetleges támadásokkal szemben.
- **Mindig ellenőrizzük, hogy rendesen bezáródott-e az összes ajtó.** Kulcs nélküli zárrendszer használata esetében ajánlott duplán megvizsgálni, hogy az autó biztonságos és a riasztó is bekapcsolt.
- **Tartsuk olyan helyen a kulcsot, ami kevésbé látható.** Nem célszerű, ha szem előtt van, mint az előszobában vagy a konyhapulton, hiszen ezzel megkönnyítjük a tolvajok feladatát.
- **Növeljük a biztonsági rétegeket.** A fizikai akadályok nagyobb hatékonysággal riasztják el a hivatlan vendégeket egyrészt a látszat, másrészt a pluszban ráfordítandó energia és idő miatt.

²⁷ u.o.

- **Állítsunk be úgynevezett „szellem indításgátlót”.** Ez egyfajta védelmi rétegnek számít, amely tulajdonképpen nem más, mint egy kód. Bizonyos autóknál lehetséges, hogy csak is a kód beírása után induljon el.
- **Nyomkövető eszköz felszerelése.** Lehetséges, hogy extra dolognak tűnik, valamint nem akadályozza meg, hogy ellopják a járművet, azonban jelentősen megnöveli annak az esélyét, hogy a rendőrség gyorsabban felderítse.²⁸ Mindemellett kedvező áron beszerezhető.

Mi történik az autóval miután ellopták? A tolvajoknak egy dologra kell figyelniük: nem állíthatják le a motort. Amint ez megtörténik nem tudják újraindítani a járművet és jelentősen nehezebbé válik a feladatuk. Elterjedt gyakorlat, hogy az elloptott gépjárművet, amint lehetséges elviszik egy szakemberhez, aki kicseréli a teljes számítógépes rendszert, ezzel új kulcs, valamint hozzáférés kerül az elkövetők kezébe. Innentől kezdve kedvük szerint használhatják az autót.

²⁸ U.O.

3. Lopásgátló eszközök

Az eredetileg, gyári biztonsági rendszerrel felszerelt gépjárművek esetében megközelítőleg másfél perc szükséges a tolvajoknak ahhoz, hogy elmozdítsák.²⁹ Annak érdekében, hogy nagymértékben meghosszabbítsuk ezt az időt, vagy elérjük, hogy az elkövetők felhagyjanak jogellenes cselekményeikkel, ajánlott utólagosan védelmi eszközöket beszerezni.³⁰ Ezek lehetnek konkrétan fizikai akadályok, valamint elektronikus blokkoló rendszerek.³¹ Az utóbbiak nagyobb védelmet garantálnak, hiszen, abban az esetben, ha a tolvaj hatástalanítani szeretné őket, mindenképpen olyan vezeték vagy vezetékek működését szükséges megszakítani, amelyek szerepet játszanak a gépjármű üzemeltetésében.³² Természetesen, ha rászánjuk magunkat, hogy ilyen utólagos védelmi, lopásgátló eszközöket szerelünk autónkba mindenképpen olyat válasszunk, amellyel a legkevesebb és legpontosan beavatkozás hajtható végre a járművön.

3.1. Fizikai akadályok

A korábbiakban már említésre kerültek a fizikai akadályok, mint a relay-támadás elleni egyik hatékony védekezés. Természetesen ezek az eszközök a hagyományos autólopás ellen is remek védelmet biztosítanak, így régebb óta alkalmazzák már az autó tulajdonosok. Elterjedésük száma ugyan nem mondható magasnak, azonban megfizethető árért olyan szolgáltatást nyújtanak, amely nagymértékben garantálja, hogy gépjárművünket abban a pozícióban találjuk meg, ahogy utoljára hagytuk. Fizikai akadályok közé tartozik többek között a kormányzár, a kuplungzár, a gázpedálzár, a sebességváltó zár, valamint a fékzár.

A felsoroltakon kívül említeném a kódpadot³³, amely hasonlít a PIN-kódos megoldáshoz. Az autó kinyitását követően a kódpad felülete világítani kezd és ide kell beírni a megfelelő számkombinációt. Általában látható helyen található és könnyen kezelhető. Különböző fajtáival találkozhatunk: vannak, amelyek nem engedik a motor elindulását a kód beírása nélkül, illetve egyes esetekben csupán megtett kilométer után jeleznek a hitelesítő kód elmaradásáról. Egyfajta negatívumként említhető, hogy a folyamatos érintés következtében egy idő után látszódní fog mely számok szerepelnek a kódban, megkönnyítve ezzel a tolvajok feladatát.

²⁹ SZAYER – KOVÁCS.: Gépjárművédelmi megoldások a..., 2019.

³⁰ u.o.

³¹ u.o.

³² u.o.

³³ MINI Guard honlapja, In: <https://dcasystem.hu/> (Megtekintve: 2024.10.17.)

3.2. Nem fizikai akadályok

Ugyan nem tekinthetőek fizikai akadálynak, azonban van olyan biztonsági rendszerek, amelyek kiváló védelmet nyújtanak. Léteznek olyanok, amelyek Bluetooth-os azonosítást követelnek, kiszűrve ezzel a nem kívánatos sofőröket. Az autóba beépített lopásgátló rendszert a mobiltelefonunkon keresztül kényelmesen és egyszerűen kezelhetjük. Az azonosítást ezesetben a mobilunk végzi, amely lehet akár a zsebünkben, akár a táskánkban. A lényeg, hogy meghatározott területen belül szükséges lennie, minél közelebb az autóhoz.³⁴

Mindemellett a fejlett rendszerek képesek arra is, hogy leállítsák az autó motorját abban az esetben, ha a sofőr nem igazolta a jogos használatot. A beépített eszköztől függően az autó vezetőjének be kell nyomnia egy elrejtett nyomógombot³⁵, vagy a fent említett Bluetooth rendszerhez hasonló módon szükséges bizonyítani jogosultságát, esetleg egy kártya érintésével.³⁶ Ha ez az azonosítás nem történik meg, vagy nem megfelelően, akkor a rendszer beindul és hangjelzéssel felhívja a sofőr figyelmét még utolsó alkalommal az igazoltatásra, majd a gépjármű lelassul és megáll. Nincs probléma akkor sem, ha az autót például szervizbe kell vinni. Mindegyik autó lopásgátló rendszerben található szerviz üzemmód.

Ha mindezek után az autó tulajdonosa továbbra sem érzi biztonságban a gépjárművét, akkor javasolt a műholdas, GPS járműkövetést szolgáltatás igénybevétele.³⁷ A tulajdonosnak elegendő egy SMS-t küldenie annak érdekében, hogy megtudja járműve pontos helyzetét, illetve extrém esetekben, hogy kérje az autó motorjának leállítását.³⁸ Riasztás esetén a központi rendszer küld egy üzenetet, amely tartalmazza a riasztás feltételezett okát, valamint az autó tartózkodási helyét.³⁹

³⁴ u.o.

³⁵ SZAYER – KOVÁCS.: Gépjárművédelmi megoldások a..., 2019.

³⁶ As Solutions honlapja, In: <https://assolutions.hu/blog/164/gepjarmuveelmi-kisokos-mi-az-immobiliser-es-az-auto-lopasgato> (Megtekintve: 2024.10.17.)

³⁷ MINI Guard honlapja, In: <https://dcasystem.hu/> (Megtekintve: 2024.10.17.)

³⁸ u.o.

³⁹ u.o.

4. Tesla

A Tesla márkájú autókat megjelenésük óta különleges helyet foglalnak el az autóiparban, és gyakran emlegetik őket a hagyományos gépjárművektől eltérő, fejlettebb technológiai színvonaluk miatt. Nem csupán arról van szó, hogy ezek az autók teljesen elektromos meghajtással közlekednek, mindemellett az innováció számos területét integrálják a járművekbe. Legyen szó például önvezető rendszerről, folyamatosan frissülő szoftverekről vagy fejlett kiberbiztonsági megoldásokról. Mindezek a jellemzők egyeduralkodó teszik a Teslákat, ugyanakkor felmerül a kérdés, hogy ezek az autók milyen mértékben különböznek más gépjárművektől, ha az eltulajdonításuk lehetőségeit vizsgáljuk. Vajon egyszerűbb vagy nehezebb ellopni egy Tesla gépjárművet, mint egy hagyományos autót?

4.1. A Tesla járművek lehetséges nyitási módjai

A Tesla járművek jelenleg három kulcstípust támogatnak: a telefonkulcs, a kulcskártya és a kulcstávírányító. Ez azt jelenti, hogy három különböző módon lehet elérni, hogy az autó zárjai feloldódjanak és a jármű elinduljon.

Elsődleges kulcsként az okostelefonok szolgálnak, amelyek egy vezeték nélküli hitelesítési folyamat, Bluetooth-kapcsolat segítségével létesítenek kapcsolatot közöttünk és az autónk között.⁴⁰ Ehhez csupán annyi szükséges, hogy a megfelelő alkalmazás le legyen töltve a telefonra (Tesla alkalmazás), valamint az eszköz a táskánkban vagy zsebünkben legyen. Ezt hívjuk telefonkulcsnak. Ha az autó, annak ellenére, hogy nálunk van a mobiltelefon, de nem nyílik ki automatikusan, még mindig van lehetőség manuálisan kinyitni, majd az alkalmazásba belépve elindítani a járművet. Továbbá nem kell megijednünk, ha az autóban marad a telefonunk, mivel nem fognak bezáródni az ajtók. Megjegyzem, a 2020 előtt gyártott (kimondottan a Model S és Model X) Tesla járművek esetében a telefonkulcs funkció nem alkalmazható.⁴¹ A távoli indításhoz ezeknél a modelleknél a hagyományos internetkapcsolat szükséges.

Kulcskártya esetében a kártyát az autó meghatározott részére kell helyezni, majd a rendszer beolvassa és megjegyzi.⁴² A kulcstávírányító, vagy hétköznapi nevén kocsikulcsnál, ugyanezt a folyamatot kell elvégezni.

⁴⁰ A Tesla járművek kulcsai, In: https://www.tesla.com/hu_hu/support/tesla-vehicle-keys (Megtekintve: 2024.09.28.)

⁴¹ u.o.

⁴² u.o.

4.2. A Tesla autók védelme

A Tesla autók esetében lehetséges a PIN-kódos védelem⁴³, azonban ez nincsen beépítve minden modellbe. Ha viszont igen, akkor mindenképpen érdemes beállítani. Lényegében annyit jelent, hogy az autó csupán egy négy számjegyből álló PIN-kód helyes megadása után fog beindulni. Ennek segítségével még, ha sikerül is bejutniuk az elkövetőknek az autó elektronikus rendszerébe, kinyitva ezzel az ajtókat, a kód megadása már problémát jelent számukra, hiszen a feltörésre használt eszköz tevékenységi köre már nem terjed ki erre.

Ugyan még csupán fejlesztések alatt van, de a Tesla a jövőben tervezi beépíteni az újabb modelljeibe az ujjlenyomattal, illetve arcfelismerés segítségével történő biztonsági rendszert. Ez annyit jelent, hogy a jármű elindításához szükséges lesz egy ujjlenyomat által hitelesített jogos hozzáférés adása.

Nagy viták folynak arról, hogy egyszerűbb vagy nehezebb-e egy Tesla autó ellopása. Technológiai szempontból jelentősen eltér, mint a hagyományos, egyszerűbb autók esetében, ahhoz pedig, hogy választ kapjunk rá meg kell vizsgálnunk az alkalmazott módszereket. Megjegyezném, hogy tolvajok szakértelme is befolyásoló tényező lehet.

Miért nehezebb ellopni egy Teslát?

- Egyrészt erősebb digitális védelemmel rendelkeznek. Ezek az autók fejlett kiberbiztonsági rendszerekkel vannak felszerelve, amelyek folyamatosan figyelik a jármű szoftveres integritását.⁴⁴ Ezenkívül, ahogy fent is említésre került, a Tesla autók rendelkeznek a PIN-kódos védelemmel (PIN to Drive), amely egy további réteget ad a biztonsághoz.⁴⁵
- Másrészt másodlagos védelmi eszközként szolgál a telefonunk, hiszen mobilalkalmazás-alapú hozzáférés szükséges a zárok kinyitásához és az autó elindításához. A Tesla-kulcs helyett gyakran applikációt használunk, ami kétfaktoros hitelesítéssel van védve. Ennek feltörése jelentős technológiai tudást igényel.
- Harmadrészt a Tesla járművek rendelkeznek valós idejű nyomkövetési opcióval.

⁴⁶ A GPS-alapú nyomkövetés segítséget nyújt a tulajdonosnak, illetve a hatóságok

⁴³ Tesla hivatalos honlapja, Biztonsági és védelmi beállítások, In: https://www.tesla.com/ownersmanual/modely/hu_hu/GUID-94B0E05E-F642-4C8E-8FED-E5EB45FA27DA.html (Megtekintve: 2024.09.28.)

⁴⁴ Tesla hivatalos honlapja, A jármű biztonsági és védelmi funkciói, In: https://www.tesla.com/hu_hu/support/vehicle-safety-security-features? (Megtekintve: 2024.12.16.)

⁴⁵ u.o.

⁴⁶ u.o.

számára annak érdekében, hogy a lehető leggyorsabban megtalálják az autót. Így ez a funkció egyben megnehezíti a jármű ellopását, valamint annak elrejtését.

- Mindemellett a szoftverek és a zárolási rendszer fejlettsége lehetővé teszi, hogy a képesek legyünk távolról deaktiválni az autót abban az esetben, ha illetéktelen személy(ek) próbálná meg használatba venni.⁴⁷

Miért lehet mégis egyszerűbb a Tesla ellopása bizonyos esetek?

- A digitális támadásokkal (kiberbűncselekményekkel) szemben a Tesla biztonsági rendszere sem képes teljeskörű védelmet nyújtani. Ha a tolvaj hozzáfér a tulajdonos Tesla-fiókjához (pl. adathalászattal vagy gyenge jelszó miatt), távolról nyithatja ki az ajtókat és indíthatja be a járművet. A bűnözők számára Bluetooth-os kommunikáció, illetve a Tesla-kulcsok rendszerének feltörése sem jelenthet problémát.
- A korábbiakban említettem a fejlett szoftvereket, valamint, hogy nagy szerepet játszanak a védelem megfelelő működésében, azonban a ritkán, de előfordulhatnak olyan hibák, „nyitva maradt kikapuk”, amelyek lehetőséget nyújtanak a tolvajok számára. Jó hír viszont, hogy a Tesla folyamatosan dolgozik ezek kiküszöbölésén.
- Itt lehet még megemlíteni a korábbiakban már részletesen kifejtett relay-támadást, amelyek szintén, voltaképpen kevesebb sikerrel lehetségesek a Tesla autók esetében is, köszönhetően a komolyabb biztonsági rétegeknek.

Annak érdekében, hogy átláthatóbb legyen az alábbi táblázatban összeszedtem a legfontosabb jellemzőket.

<i>Miért nehezebb?</i>	<i>Miért egyszerűbb?</i>
Erősebb digitális védelem	Digitális támadások
Mobilalkalmazás-alapú hozzáférés	Szoftveres sebezhetőségek
Valós idejű nyomonkövetés	Relay-támadások
Szoftver és tárolási rendszer fejlettsége	

1.táblázat: Miért nehezebb és miért egyszerűbb a Tesla autók ellopása? (saját szerkeztés)

⁴⁷ u.o.

Mindezeket figyelembe véve véleményem szerint egy Tesla ellopása általában nehezebb, mivel a gyártó komoly technológiai védelmet épített be, amely csökkenti a sikeres lopás esélyét. Ugyanakkor, ha a tolvajok kifejezetten a Tesla-k ellopására specializálódtak, illetve képesek kijátszani a digitális rendszereket, akkor ugyanazzal a technikával, az információs rendszer kijátszásával, ezek a módszerek hatékonyabbak lehetnek, mint egy egyszerűbb autóval szembeni mechanikus támadása. Megfigyelhető azonban, hogy összességében kevesebbet lopnak el belőle.

4.3. Etikushacker-verseny, ahol mindenki nyer

Néhány éve rendszeresen megrendezésre kerül Vancouverben, Kanadában az úgynevezett Pwn2Own infobiztonsági verseny.⁴⁸ A Tesla által meghirdetett megmérettetés lényege, hogy a résztvevő hackerek különleges feladatot kapnak: fel kell törniük egy Tesla Model 3 szoftverének védelmi rendszerét.⁴⁹

A tavalyi évben, 2023. tavaszán történt, hogy egy francia hackerekből álló csapatnak sikerül kevesebb, mint pár perc alatt bejutniuk az autó rendszerébe, átvéve ezzel a biztonsági és kényelmi funkciók feletti irányítást.⁵⁰ Ez az első kiskapu csak a kezdet volt. A Tesla embereit is meglepték, mikor sikerült bejutniuk az autó vezérlőelektronikájába az infotainment rendszerének Bluetooth vezérlőjén keresztül.⁵¹

A hackerek számára motivációként szolgál, hogy ha sikerül bármilyen rendszerbeli problémát (kiskapukat) észlelniük, akkor jutalmat kapnak. A francia csapat sem tért haza üres kézzel: egy Teslával, illetve 350 ezer dollárral lettek gazdagabbak.⁵² Az elmúlt években a Tesla egyre nagyobb figyelmet fordít az autó kiberbiztonsági fejlesztésére és emiatt is fontos számukra, hogy évente ellenőrizték mennyit sikerül fejlődniük.

Az egyik legfontosabb indok a megbízható védelemi rendszer kiépítésére: annak feltörése, és ennek következtében a jármű feletti irányítás átvétele kiszámíthatatlan és súlyos baleseteket okozhat, valamint az utasok életét és testi épségét is jelentősen veszélyezteti.⁵³

⁴⁸ Két perc alatt feltörték egy Tesla rendszerét a hacker versenyen, In: <https://www.autonavigator.hu/cikkek/ket-perc-alatt-feltortek-egy-tesla-rendszeret-a-hacker-versenyen/> (Megtekintve: 2024.10.06.)

⁴⁹ A Tesla versenyt rendezett a hackerek számára. A győztes autót kapott, In: <https://www.letemsvetemapple.eu/hu/2019/03/25/tesla-poradala-soutez-pro-hackery-vitez-dostal-auto/> (Megtekintve: 2024.10.06.)

⁵⁰ Két perc alatt feltörték egy Tesla rendszerét a hacker versenyen, In: <https://www.autonavigator.hu/cikkek/ket-perc-alatt-feltortek-egy-tesla-rendszeret-a-hacker-versenyen/> (Megtekintve: 2024.10.06.)

⁵¹ u.o.

⁵² u.o.

⁵³ A Tesla versenyt rendezett a hackerek számára. A győztes autót kapott, In: <https://www.letemsvetemapple.eu/hu/2019/03/25/tesla-poradala-soutez-pro-hackery-vitez-dostal-auto/> (Megtekintve: 2024.10.06.)

5. Lopás vs. az információs rendszer vagy adat megsértésének bűncselekménye

Ahhoz, hogy el tudjuk dönteni melyik bűncselekmény valósul meg a modernkori gépjárműlopás esetében, szükséges mindkét deliktumot alaposan megvizsgálni. Indokolt foglalkozni továbbá azokkal a meghatározó jellemzőkkel, tényezőkkel, egyedi tulajdonságokkal, amelyek választ adhatnak a kérdésekre.

5.1. Lopás

A lopást a Btk. vagyon elleni bűncselekmények fejezetében találjuk meg, pontosabban a 370. § rendelkezik róla. Eszerint „aki idegen dolgot mástól azért vesz el, hogy azt jogtalanul eltulajdonítsa, lopást követ el”. Angyal Pál szerint egy vagyon ellen irányuló bűncselekményről beszélhetünk, amely valamely jogilag védett szubjektív vagyoni érdeknek jogellenes megzavarására irányul.⁵⁴ A védett jogi tárgya tehát a tulajdonjog, amelyet az elkövető a birtoklási jog elvonásával sért meg.⁵⁵

Az (1) bekezdés egyfajta definícióként is tekinthető, ebből kifolyólag fontosnak tartom az egyes szavak tágabb értelmezését. A deliktum elkövetési tárgya minden esetben dolog, amely egyrészt ingó, másrészt idegen, harmadrészt pedig meghatározott értékkel kell rendelkeznie.⁵⁶

Egyes esetekben nehézségeket okoz meghatározni mi tekinthető dolognak, azonban a Polgári Törvénykönyv (továbbiakban: Ptk.) irányadó szabályai alapján minden olyan birtokba vehető testi tárgy ide sorolható, amely tulajdonjog tárgya lehet⁵⁷. Megfogható és az ember által elérhető. Mivel a lopás csak mozdítható tárgyakra követhető el, ezért a bűncselekmény kizárólag ingó dolog ellen irányulhat, ingatlan szóba sem jöhet. Ami a dolog idegenségét illeti, teljesen az elkövető tulajdonán kívülállónak kell lennie, mivel, ha csupán részben is, de tulajdonosi joggal rendelkezik a dolog felett, cselekménye már nem számít deliktumnak. Másik fontos kritérium, hogy a dolog nem lehet uratlan, valakinek a tulajdonában vagy birtokában kell, hogy álljon. Megjegyezném, hogy jogtalan birtokostól is lehet lopni, tehát a bűncselekmény akkor is megvalósul, ha az autót utóbb a tolvajtól is eltulajdonítja egy harmadik személy.⁵⁸

⁵⁴ ANGYAL Pál: A lopás. A magyar büntetőjog kézikönyve 10. Athenaeum, Budapest, 1933, 17. o.

⁵⁵ BELOVICS Ervin (szerk.): Büntetőjog II. Különös Rész. HVG-Orac Lap- és Könyvkiadó, 2021, 708. o.

⁵⁶ u.o.

⁵⁷ Ptk. 5:14 § (1) bek.

⁵⁸ BELOVICS (szerk.): Büntetőjog II. Különös..., 709. o.

A deliktum esetében kiemelt figyelmet kap a dolog értéke is, hiszen egyrészt ez határozza meg, hogy a bűncselekmény alap vagy minősített esete következett be, esetleg szimpla szabálysértési alakzat állapítható meg. Abban az esetben tehát, ha a lopás befejezett stádiumba kerül, a ténylegesen eltulajdonított értéket kell figyelembe venni a bűncselekmény minősítése szempontjából, azonban ebbe nem számítható bele az okozott kár értéke, ha a lopás dolog elleni erőszakkal elkövetettnek minősül.⁵⁹ Az érték nem más, mint a dolognak az elkövetés időpontjában meglévő, pénzben kifejezett forgalmi értéke.⁶⁰ A lopás érték szerinti meghatározásakor mindig a dolog kiskereskedelmi árát kell figyelembe venni.⁶¹

A lopás esetében az elkövetési magatartás nem más, mint az elvétel, amely két különböző mozzanatból áll. Először a dolog kikerül a birtokos tényleges rendelkezési köréből, majd ezt követően az elkövető létrehozza saját birtokos állapotát.⁶² Ebből következik, hogy mindaddig, amíg az elvételnek csak az első mozzanata valósul meg, tehát a dolog elmozdítása, csupán a lopás kísérlete állapítható meg. A bírói gyakorlat megjegyezte, hogy az elvétel következtében a dolog korábbi birtokosa nem lesz abban a helyzetben, hogy a dolog felett a továbbiakban is hatalmat gyakoroljon, valamint azzal rendelkezzen.⁶³

Immateriális bűncselekmény, vagyis nincsen eredménye.⁶⁴ Ebből következik, hogy közömbös a büntetőjogi felelősségre vonás szempontjából, hogy a deliktum sikeres volt-e. Elegendő az elkövető birtokállapotának létrejötte a befejezett alakzathoz.⁶⁵ Közömbös továbbá, hogy a bűncselekmény megvalósulása után mi történik a dologgal. Így abban az esetben, ha a tolvaj az ellopott gépjárművet az üldözés közben az út szélén hagyja és elmenekül, a lopás tényállását mindettől függetlenül megvalósította. A lopást ugyanis anyagi jogi értelemben úgy kell értelmezni, minthogyha az elvétel megvalósulásával a dolog megsemmisülne, nem lenne többé.⁶⁶

A jogszabály nem bünteti az előkészületi szakaszt, azonban különbséget lehet tenni ezesetben az általános lopás, illetve a dolog elleni erőszakkal elkövetett lopás között. Az utóbbi a lopás egyik elkövetési módja, ezért súlyosabb büntetést von maga után. Az autólopás esetén dolog elleni erőszakkal elkövetett lopásról beszélhetünk, amely mindaddig nem büntetendő,

⁵⁹ AMBRUS István – MEZEI Kitti – MOLNÁR Erzsébet: Magyarázat a compliance jogszabályairól I. – Általános és büntetőjogi compliance, Wolters Kluwer Hungary, Budapest, 2021, 188. o.

⁶⁰ BELOVICS (szerk.): Büntetőjog II. Különös..., 709. o.

⁶¹ u.o.

⁶² AMBRUS – MEZEI – MOLNÁR: Magyarázat a compliance jogszabályairól..., 181. o.

⁶³ EBH 2012.B.32.

⁶⁴ AMBRUS – MEZEI – MOLNÁR: Magyarázat a compliance jogszabályairól..., 182. o.

⁶⁵ BELOVICS (szerk.): Büntetőjog II. Különös..., 711. o.

⁶⁶ u.o.

amíg a tolvaj nem fejt ki olyan tevékenységet, amely a jármű elvételére irányulna.⁶⁷ Ahogyan azt a korábbiakban már említettem a kísérleti szakról akkor beszélhetünk, ha az elkövetési magatartásnak, vagyis az elvételnek csupán az első mozzanata valósul meg (például az elkövető elkezd eszköz segítségével kinyitni az autó ajtaját).⁶⁸ Ebben az esetben vizsgálni kell, hogy az elkövető szándéka milyen érték ellopására irányult⁶⁹, hiszen ez fogja meghatározni a kiszabható büntetést. Megjegyezném, hogy – mint általában a kísérleti szakaszban – lehetséges a bűncselekmény elkövetésétől való önkéntes elállás, azonban a bírói gyakorlat szerint ez csupán akkor vehető figyelembe, ha az elkövető belső készítésre hagy fel a tevékenységével, és nem külső körülmények (például zavaró tényezők, komolyabb védelmi rendszer) hatására.⁷⁰

A lopás deliktuma alanyi oldalon célzatos, tehát mindenképpen szándékosan, valamilyen dolog elvételére irányuló magatartás.⁷¹ A célzat pedig nem más, mint a jogtalan eltulajdonítás, vagyis a tolvaj a véglegesség szándékával maga kívánja gyakorolni a tulajdonost megillető jogosítványokat (mint például a birtoklás vagy a használat), természetesen mindezt jogellenesen.⁷² Fontos kiemelni, hogy nem feltétele a lopás befejezetté válásának, hogy az elkövető az eltulajdonított dolgot utána használja vagy esetlen értékesítse.⁷³

Mint azt már említettem, a gépjárműlopás esetén a dolog elleni erőszak a deliktum elkövetési módja, amelyhez általában – de nem kötelező jelleggel – állagsérelem, valamint a dologra irányuló, jelentős erő kifejtés társul.⁷⁴ Ebből kifolyólag mindenképpen szükség van arra, hogy megvalósuljon egy fizikai ráhatás akár a dolog, akár annak védelmére szolgáló berendezés ellen, de semmiképpen sem irányulhat személlyel szemben. Így, ha az elkövető az autót nyitott ajtókkal találja, benne az indításhoz szükséges kulccsal vagy kulcskártyával, nem valósulhat meg a lopás minősített esete, azonban, ha a lezárt gépkocsi résnyire nyitva hagyott ablakát lenyomja, akkor már kimeríti a tényállást⁷⁵. A dolog elleni erőszakkal elkövetett lopás esetén ún. összetett bűncselekményről beszélhetünk, amely magában foglalja egyrészt a rongálás deliktumát, mint eszközcselekményt, másrészt a dolog elvételét (a lopást), mint az egésznek a célcselekménye. Az összetett törvényi tényállás megalkotásának indoka az alaptényállások között fennálló szoros cél-eszköz viszony.⁷⁶

⁶⁷ BH 2017.257.

⁶⁸ BELOVICS (szerk.): Büntetőjog II. Különös..., 711. o.

⁶⁹ 11. BK vélemény

⁷⁰ BH 2004.271.

⁷¹ AMBRUS – MEZEI – MOLNÁR: Magyarázat a compliance jogszabályairól..., 187. o.

⁷² u.o.

⁷³ u.o.

⁷⁴ AMBRUS – MEZEI – MOLNÁR: i.m., 188. o.

⁷⁵ BH 1993.142.

⁷⁶ BELOVICS Ervin: Büntetőjog I. Általános Rész. HVG-Orac Lap- és Könyvkiadó. 2020. 395. o.

5.2. Információs rendszer vagy adat megsértése

A hálózati bűncselekmények csoportjába tartozó, valamint a kiberbűncselekmények közül a leggyakrabban előforduló információs rendszer vagy adat⁷⁷ megsértésének deliktuma nem véletlenül vetődik fel az újfajta gépjárművek eltulajdonítása esetén, mint lehetséges megvalósult bűncselekmény. Ahogy a korábbiakban már említettem, ezeknél az autóknál az információs rendszer játszik központi szerepet, így a tolvajok ezt veszik célba.

Az elkövető magatartása az információs rendszer és az abban tárolt adatok ellen irányul.⁷⁸ Egyrészt megnyilvánulhat a rendszerbe történő jogosulatlan belépéssel és egyben a védelmet biztosító program megsértésével vagy kijátszásával, másrészt a belépési jogosultság kereteit túllépve vagy azt megsértve való bent maradással.⁷⁹ Az első változat valósul meg például a relay-támadások esetén, mikor is az elkövető, a kezében lévő eszköz segítségével átveri, kijátssza a gépjármű biztonsági rendszerét, melynek eredményeként az autó feloldja a zárat és beindul a motor. Ezesetben az autó úgy érzékeli, hogy nem történt semmi szokatlan vagy jogellenes behatolás, így nem kezd el hangot, illetve fényjelzést adni.

A bűncselekmény megvalósulásához szükséges a védelmet biztosító technikai intézkedés megsértése vagy annak kijátszása (amely a „hagyományos” autólopás esetén egyet jelent a riasztó kiiktatásával), mivel önmagában a jogosultság keretein való átlépés nem éri el a szükséges veszélyességi szintet.⁸⁰ A rendszerbe történő jogosulatlan belépés (ún. hackelés következtében) a bűncselekmény enyhébben büntetendő alapesetét valósítja meg, azonban a belépés nem lehet jogosulatlan, ha az információs rendszer nincsen levédve, vagy az nincs aktiválva.⁸¹ Tehát abban az esetben, ha figyelmetlenségből nem zárjuk be az jármű ajtajait, nem valósulhat meg az elsőként említett, információs rendszer védelmét biztosító rendszer megsértése vagy kijátszása.

Elkövetési tárgy egy meghatározott dolog, személy vagy esetlen más speciális tárgy, amelyre vagy akire az elkövetési magatartás irányul.⁸² Más speciális tárgy alatt értjük a kézzel nem fogható, virtuális tárgyakat, amelybe bele tartozik az információs rendszerben található

⁷⁷ A Btk. 423. § (5) bekezdés értelmében: adat az információs rendszerben tárolt, kezelt, feldolgozott vagy továbbított tények, információk vagy fogalmak minden olyan formában való megjelenése, amely információs rendszer általi feldolgozásra alkalmas, ideértve azon programot is, amely valamely funkciónak az információs rendszer által való végrehajtását biztosítja.

⁷⁸ BELOVICS: Büntetőjog II. Különös..., 1006. o.

⁷⁹ Btk. 423. § (1) bek.

⁸⁰ BH 2017.392.

⁸¹ GRUND Borbála: A kibertér bűncselekményeiről és a kiberbűnözés hazai gyakorlatáról. In: MTA Law Working Papers, 2021/21. szám, 14. o.

⁸² GELLÉR Balázs – AMBRUS István: A magyar büntetőjog általános tanai I. Második kiadás. ELTE Eötvös, Budapest, 2019, 204-206. o.

adat is.⁸³ Erre a megkülönböztetésre azért van szükség, mert léteznek olyan élettelen tárgyak a Btk. rendszerében, amelyek egyedi törvényi meghatározás folytán nem tartoznak a dolog büntetőjogi fogalma körébe.⁸⁴

A büntetőjogi felelősségre vonásnak nem feltétele, hogy az elkövetési magatartás károkozási, haszonszerzési vagy hasonló célzattal valósuljon meg, vagyis nem célzatos bűncselekmény. Nem tekinthető továbbá kritériumnak az sem, hogy az elkövető a későbbiekben bármilyen tevékenységet végezzen a rendszerben, vagy annak működését nehezítse, akadályozza.⁸⁵

A továbbiakban egy táblázat segítségével szeretném összegezni, melyek azok a lényeges tényezők, illetve jellemzők mindkét bűncselekmény esetén, amelyek támpontot adhatnak a megválaszolandó kérdések kapcsán.

Dolog elleni erőszakkal elkövetett lopás		Információs rendszer vagy adat megsértése
Vagyon elleni bűncselekmény	<i>Milyen kategóriába tartozik?</i>	Hálózati bűncselekmények csoportjába tartozik
Idegen, ingó, értékkel bíró dolog elvételére irányul	<i>Mi ellen irányul?</i>	Információs rendszer és az abban tárolt adatok ellen irányul
A dolog kikerül a birtokos tényleges rendelkezési köréből, majd az elkövető létrehozza saját birtokos állapotát	<i>Mi történik?</i>	A rendszerbe történő belépés és a védelmi rendszer kijátszása, megsértése
Dolog elleni erőszak megvalósulása, amely általában állagsérelemmel jár	<i>Történik-e kár?</i>	A deliktum megvalósulásához állagsérelem nem társul

2. táblázat: A dolog elleni erőszakkal elkövetett lopás és az információs rendszer vagy adat megsértésének összehasonlítása (saját szerkeztés)

⁸³ AMBRUS – MEZEI – MOLNÁR: Magyarázat a compliance jogszabályairól..., 326. o.

⁸⁴ MEZEI Kitti: A kiberbűnözés szabályozási kihívásai a büntetőjogban, In: *Ügyészek Lapja*, 26: 4-5. pp. 21-33., 13.p., (2019)

⁸⁵ AMBRUS – MEZEI – MOLNÁR: i. m., 327. o.

5.3. A bűncselekmény minősítésének dogmatikai kérdései

Az autólopás jogi megítélése jelentős kihívást jelent a modern technológiai környezetben. Kulcsfontosságú lenne a hatóságok számára tisztázni, hogy milyen deliktumok valósulnak meg egy ilyen cselekmény elkövetése során. A modern autók ellopása esetén ugyanis felmerül a korábbiakban már említett lopás minősített esete, a dolog elleni erőszakkal elkövetett lopás, valamint az információs rendszer vagy adat megsértésének bűncselekménye. Mindezek értelmezése és alkalmazása azonban nem egyértelmű, így nagymértékű eltérések figyelhetők meg a gyakorlatban.

A bűncselekmény pontos jogi megítélését csak a törvényi tényállás alapos vizsgálatával lehet megállapítani. A problémát a gyökerénél kell megragadni, vagyis a jogalkalmazók számára az elsődleges kérdés az, hogy a modern technológiával végrehajtott autólopás mely törvényi tényállások alá sorolható be. Ezen a téren azonban jelentős eltérések figyelhetők meg, mind a joggyakorlatban, mind a jogirodalomban. Ugyanez megfigyelhető az ügyészség és a bíróság között is, gyakran eltérő értelmezések alakulnak ki.

Az ügyészség gyakran abból indul ki, hogy a gépjármű eltulajdonításának megakadályozására szolgáló biztonsági rendszer hatástalanítása dolog elleni erőszaknak minősül.⁸⁶ Ide sorolható például az az eset is, amikor az elkövető külső elektronikai eszköz segítségével teszik alkalmatlanná a biztonsági rendszert. Az ügyészség szerint minden olyan cselekmény, amely a biztonsági rendszer működésének ellehetetlenítésére irányul, erőszakos módon elkövetett bűncselekményként értékelhető.

A relay-támadások esetében azonban más a helyzet. Az ilyen esetekben az elkövetők nem teszik működésképtelenné a biztonsági rendszert. Ellenben kihasználják annak működését. Ez annyit jelent, hogy az elkövetők célja nem a rendszer alkalmatlanná tétele, mivel annak megtévesztésére játszanak. A relay-támadás során az autó biztonsági rendszerét „átverik” annak érdekében, hogy jogosulatlan hozzáférést szerezzenek, miközben magát a rendszert érintetlenül hagyják. Mondhatni a tolvajoknak „szükségük van a rendszer működésére”. Ebből adódóan az ilyen cselekmények nyom nélkül végrehajthatóak, ami további kihívást jelent a hatóságok számára.

Felmerül a kérdés: beszélhetünk-e hachelésről a relay-támadások esetében? Meglátásom szerint igen, mivel a tolvajok valójában az autó információs rendszerébe hatolnak be. A

⁸⁶ Btk. 370. § (2) bek. bc) pont: A büntetés vétség miatt két évig terjedő szabadságvesztés, ha dolog elleni erőszakkal – ideértve azt is, ha dolog eltulajdonításának megakadályozására szolgáló eszközt állagsérelem okozása nélkül eltávolítják, vagy a dolog eltulajdonításának megakadályozására alkalmatlanná teszik – követik el.

rendszerbe történő jogosulatlan behatolása során megváltoztathatják a járműben lévő adatokat azáltal, hogy úgymond lopott hitelesítési adatokat közvetítenek tovább. Ez egyértelműen megfelel a hachelés fogalmának, hiszen az elkövetők manipulálják az autó információs rendszerét a saját céljaik elérése érdekében.

Fontos hangsúlyozni, hogy mindezek miatt a relay-támadásokkal végrehajtott autólopások nem sorolhatóak be a dolog elleni erőszakkal elkövetett lopás törvényi tényállása alá. Ez azzal magyarázható, hogy az elkövetők nem teszik működésképtelenné a biztonsági rendszert, csupán megtevesztik azt. Így a hagyományos lopási megfogalmazásba nem tartoznak bele ezek az esetek. Szükség van a jogi keretek újragondolására és tágabb értelmezésére.

Összefoglalva tehát a relay-támadásokkal végrehajtott autólopások egy új típusú deliktumot foglalnak magukba, amelyek jogi értelmezése és minősítése jelentős kihívás elé állítja a bíróság mellett az ügyészséget, valamint a nyomozó hatóságot is. Az ilyen bűncselekmények pontos megítélése érdekében elengedhetetlen a törvényi tényállások korszerűsítése és az információs rendszer elleni deliktumok pontos definiálása. Ez nem csak a hatóságok munkáját könnyítené meg, hanem a jogbiztonságot is növelné, miközben hozzájárulna a technológiai fejlődés által generált új kihívások hatékony kezeléséhez.

6. Következtetések

Hiába próbáljuk távol tartani magunkat a technika követheetlen változásaitól, a kibertér megállíthatatlan terjeszkedésétől a kiberbűncselekmények szinte minden területen megjelennek. Így van ez az a gépjárműlopás esetében is. Ahogy már korábban is említésre került, manapság az autók többségének irányításáért és védelméért a beépített információs rendszer felel⁸⁷, amely kulcsfontosságú szerepet kap mindkét oldalon. A járműnek szüksége van rá, hogy működni tudjon, az elkövetők számára pedig ez jelenti a bejutási pontot anélkül, hogy kárt tennének az autóban. Egyszerűbb, gyorsabb, valamint „tisztább” elkövetés.

Továbbra is dolog elleni erőszakkal elkövetett lopásnak minősül, ha ezeket az autókat kézzel, illetve segédeszközzel (például hamis kulccsal, feszítővassal) törik fel. Azonban, ha az információs rendszeren keresztül, például jogosulatlan adatbevitellel vagy a rendszer átprogramozásával (ún. hackeléssel) sikerül kinyitni az ajtókat, egyértelműen az információs rendszer vagy adat megsértésének törvényi tényállása valósul meg. Mindebből következően egyetértek azzal az állásponttal, hogy az információs rendszer vagy adat megsértésének, valamint – nem dolog elleni erőszakkal elkövetett lopás, hanem – a célba vett gépjármű értékének megfelelő minősítésű lopás valószínű bűnhalmazatban való megállapítására köteles a bíróság.⁸⁸ A valószínű bűnhalmazat azt jelenti, hogy az elkövető egyidejűleg több bűncselekményt is megvalósít, azonban ezeket egy eljáráson belül bírálják el. Ebben az esetben a lopás büntette a célcselekmény és ennek eszközcselekményeként szolgál az információs rendszer vagy adat megsértésének deliktuma, pontosabban az adat jogosulatlan megváltoztatása.⁸⁹

Miután megtörtént az eset minősítése és megállapítottuk milyen bűncselekmény valósult meg (ezzel megválaszolva az első nagy kérdést) jön a következő, egy fokkal nehezebb lépés: hogyan lehet mindezt bizonyítani? A kiberbűncselekmények elleni nyomozás egyik legbonyolultabb része annak feltérképezése, hogy ki és hogyan jutott be az információs rendszerbe, valamint milyen tevékenységeket végzett a bent tartózkodása alatt. A visszakövethetőség egy hosszadalmas folyamat, amely nem minden esetben szokott eredményre vezetni. Ezért is érthető miért ragaszkodik annyira az ügyészség a dolog elleni erőszakkal elkövetett lopás tényállásához. Nagyon nehéz bizonyítani.

⁸⁷ AMBRUS – MEZEI – MOLNÁR: Magyarázat a compliance jogszabályairól..., 189. o.

⁸⁸ AMBRUS – MEZEI – MOLNÁR: i. m., 190. o.

⁸⁹ u.o.

Ahhoz, hogy bizonyítani lehessen hogyan történt a bűncselekmény, mindenképpen szakértői véleményére van szükség, aki igazolni tudja, hogy tényleg az információs rendszerben történő változások következtében oldódott fel a zár, valamint, hogy a rendszer kijátszásával sikerült a tolvajnak eltulajdonítania a gépjárművet. Véleményem szerint ez az egyik legfontosabb lépés és egyben a döntő bizonyíték az eljárás során.

Végezetül összefoglaltam egy táblázatban a gépjárművek kiberbiztonsági fenyegetésekkel kapcsolatos információkat kiegészítve néhány olyan tényekkel, amelyekkel a dolgozatomban nem tértem ki, azonban fontosnak találtam említést tenni róluk.

Típus	Jellemző fenyegetés	Előfordulási arány	Védekezési javaslatok
Kulcs nélküli beléptetés	Relay-támadás (jel meghosszabbításával)	Az autólopások jelentős részét teszik ki, különösen kulcs nélküli autóknál	Faraday-tasak használata, kulcsrendszer kikapcsolása
Szoftveres sebezhetőségek	Távoli hozzáférés, járműrendszerek vezérlése	Okosautók elterjedésével növekszik	Rendszeres szoftverfrissítés, megbízható hálózatok használata, jelszóvédelem
Adatvédelmi kockázatok	Helyadatok, vezérlési szokások, személyes adatok illetéktelen hozzáférése	Az adatszivárgások száma növekszik, mivel az autók egyre több adatot gyűjtenek	Adatvédelemre optimalizált beállítások, adatok biztonságos tárolása és törlése
Mobilalkalmazások sebezhetősége	Távoli vezérlés és adatlopás a kapcsolódó alkalmazásokon keresztül	Az alkalmazások számának növekedésével párhuzamosan egyre nagyobb célpontot jelentenek	Biztonságos alkalmazások használata, erős jelszavak, kétfaktoros hitelesítési rendszerek alkalmazása
Hackertámadások	Átfogó támadások a jármű teljes rendszerére	Világszerte egyre gyakoribb, különösen a fejlett technikákat alkalmazó autók esetében	Gyártók által biztosított kiberbiztonsági megoldások használata

3. táblázat: A gépjárművek kiberbiztonsági fenyegetései (saját szerkeztés)

7. Irodalomjegyzék

Jogszabályok

11. BK vélemény

2012. évi C. törvény a Büntető Törvénykönyvről

2013. évi V. törvény a Polgári Törvénykönyvről

BH 1993.142.

BH 2004.271.

BH 2017.257.

BH 2017.392.

EBH 2012.B.32.

Könyvek

AMBRUS István – MEZEI Kitti – MOLNÁR Erzsébet: Magyarázat a compliance jogszabályairól I. – Általános és büntetőjogi compliance, Wolters Kluwer Hungary, Budapest, 2021, 181-182.o, 188-190. o., 326-327.o.

ANGYAL Pál: A lopás. A magyar büntetőjog kézikönyve 10. Athenaeum, Budapest, 1933, 17. o.

BELOVICS Ervin: Büntetőjog I. Általános Rész, HVG-Orac Lap- és Könyvkiadó, 2020, 395. o.

BELOVICS Ervin (szerk.): Büntetőjog II. Különös Rész. HVG-Orac Lap- és Könyvkiadó, 2021, 708-709. o., 711.o. 1006. o.

GELLÉR Balázs – AMBRUS István: A magyar büntetőjog általános tanai I. Második kiadás. ELTE Eötvös, Budapest, 2019, 204-206. o.

Tanulmányok

JAMES Hayes: Hackers under the hood: It's been five years since the first reports of car hacking emerged, but despite progress in vehicle protection standards, automotive cyber-security remains on high alert, E&T Magazine, Volume 15, Issue 03, 2020, page 32.

MIKEL Longman: The problem of auto theft, In: Forensic Investigation of Stolen-Recovered and Other Crime-Related Vehicles, pp.2., 2016

SZAYER Géza – KOVÁCS Bence: Gépjárművédelmi megoldások a modern lopási módszerek ellen, Recent Innovations in Mechatronics 6: 1 pp. 1-6., 6.p., 2019.

Folyóiratcikk

GRUND Borbála: A kibertér bűncselekményeiről és a kiberbűnözés hazai gyakorlatáról. In: *MTA Law Working Papers*, 2021/21. szám, 14. o.

LADVÁNSZKY János: Az autólopás elleni védekezés egy lehetséges módszere (kulcs nélküli indítórendszeres gépkocsik esetén), In: *Híradástechnika*, 57. Évfolyam, 2002/5. sz., 55. o.

MEZEI Kitti: A kiberbűnözés szabályozási kihívásai a büntetőjogban, In: *Ügyészet lapja*, 26: 4-5. pp.21-33., 13.p. (2019)

Internetes források

As Solutions honlapja, In: <https://assolutions.hu/blog/164/gepjarmuveelmi-kisokos-mi-az-immobiliser-es-az-auto-lopasgatlo> (Megtekintve: 2024.10.17.)

A Tesla járművek kulcsai, In: https://www.tesla.com/hu_hu/support/tesla-vehicle-keys (Megtekintve: 2024.09.28.)

A Tesla versenyt rendezett a hackerek számára. A győztes autót kapott, In: <https://www.letemsvetemapplem.eu/hu/2019/03/25/tesla-poradala-soutez-pro-hackery-vitez-dostal-auto/> (Megtekintve: 2024.10.06.)

Két perc alatt feltörték egy Tesla rendszerét a hacker versenyen, In: <https://www.autonavigator.hu/cikkek/ket-perc-alatt-feltortek-egy-tesla-rendszeret-a-hacker-versenyen/> (Megtekintve: 2024.10.06.)

Keyless car theft: What is a relay attack, how can you prevent it, and will your car insurance cover it?, In: <https://leasing.com/guides/relay-car-theft-what-is-it-and-how-can-you-avoid-it/> (Megtekintve: 2024.10.06.)

MINI Guard honlapja, In: <https://dcasystem.hu/> (Megtekintve: 2024.10.17.)

NAIR, VINAY Unnikrishnan: Smart car hacking: a threat to the rising automotive industry, In: <https://esource.dbs.ie/server/api/core/bitstreams/e87a1b88-c877-458a-a5ca-867fb09f51de/content> (Megtekintve: 2024.10.07.)

Tesla hivatalos honlatja, A jármű biztonsági és védelmi funkciói, In: https://www.tesla.com/hu_hu/support/vehicle-safety-security-features? (Megtekintve: 2024.12.16.)

Tesla hivatalos honlapja, Biztonsági és védelmi beállítások, In: https://www.tesla.com/ownersmanual/modely/hu_hu/GUID-94B0E05E-F642-4C8E-8FED-E5EB45FA27DA.html (Megtekintve: 2024.09.28.)

Zs+u honlapja, Indításgátlók, In: https://zs.uhu.hu/autoelektronika-inditasgatllok?srsltid=AfmBOoqVru8IRTjX21bdra8Pij4sxnWVlJQj8L1SDXMEzM_DOZvvcWtH (Megtekintve: 2024.10.31.)