Revija za kriminalistiko in kriminologijo / Ljubljana 69 / 2018 / 3, 215–231

Pametni avtomobili in kibernetska kriminaliteta[1]

Blaž Markelj[2], Gašper Školc[3], Vanja Ida Erčulj[4], Sabina Zgaga[5]

V preteklosti smo o avtomobilih govorili zgolj kot o prevoznem sredstvu, katerega središče sta bila voznik in avtomobil ter njuna interakcija znotraj ostalega prometa. Pri zagotavljanju varnosti je bila pomembna voznikova sposobnost vožnje v različnih razmerah in tehnična dovršenost avtomobila. S korakom naprej v razvoju tehnologije pa je avtomobil postal del interneta stvari. Avtomobil je postal sredstvo, ki se povezuje v kibernetski prostor, deluje na podlagi podatkov, ki jih sprejema iz okolice, in se povezuje z ostalimi pametnimi napravami (npr. mobilnimi napravami). S tovrstnim razvojem je avtomobil postal tudi »odprt« za kibernetsko kriminaliteto. S povezljivostjo v kibernetski prostor je postal avtomobil odprt tudi za grožnje, ki pretijo napravam v kibernetskem prostoru. Namen prispevka je prikazati varnost uporabnikovih podatkov pri rabi pametnih avtomobilov, poudariti poznavanje tovrstne problematike med uporabniki pametnih avtomobilov (tako zasebnih kot poslovnih) ter predstaviti nekatere kazenskopravne vidike te problematike. V prvem delu prispevka so predstavljena informacijskovarnostna vprašanja, vezana na pametne avtomobile, ki se dotikajo tudi kazenskopravnih elementov. Predstavljene so grožnje, ki so pogoj za uresničitev kibernetske kriminalitete. V drugem delu prispevka pa so predstavljeni rezultati raziskave, ki kažejo, kako dobro sodelujoči v raziskavi poznajo informacijsko varnost pri povezavi s pametnimi avtomobili.

Ključne besede: pametni avtomobili, mobilne naprave, informacijska varnost, kibernetska kriminaliteta, kazenska odgovornost

UDK: 004.056:629.331

1 Uvod

Vpliv razvoja tehnologije na posameznika in družbo se kaže tudi skozi načine, kako posameznik oziroma družba spreminja način dela in posledično potek življenja. Ljudje smo v današnjih časih nenehno izpostavljeni neustavljivemu razvoju tehnologije na mnogih področjih. Ko govorimo o razvoju tehnologije, vedno več govorimo tudi o avtomobilski industriji in ne več samo o računalništvu, industrijski tehnologiji, mobilnih napravah itd. Ravno tako, ko govorimo o varnosti, ne govorimo več zgolj o fizični varnosti, temveč o različnih vidikih varnosti, ki se izražajo skozi različno problematiko. V zadnjem obdobju je to kibernetska varnost in z njo povezana kibernetska kriminaliteta. Že leta 2011 Bernik in Meško (2011) v svoji raziskavi ugotavljata posameznikov strah pred kibernetsko kriminaliteto. Z večanjem rabe kibernetskega prostora in z njim povezane tehnologije se povečuje tudi tveganje uresničitve kibernetske kriminalitete. V zadnjih nekaj letih lahko opazimo velik napredek, predvsem na področju vključevanja interneta stvari (angl. *Internet of Things* [IoT]) v avtomobile (Meola, 2016). Pacheco, Satam, Hariri, Grijalvy in Berkenbrock (2016) navajajo, da se IoT povezuje tako z mobilnimi napravami in računalniki kot tudi s pametnimi mesti, domovi, drugimi pametnimi avtomobili ter drugimi deli kritične infrastrukture. Prav vključevanje omenjene tehnologije je pripeljalo do soočanja z novim pojmom pametni avtomobili. V mnogih literaturah lahko najdemo veliko število različnih definicij pametnega avtomobila, vendar nobena od teh ni uradno splošno sprejeta (European Union Agency For Network And Information Security [ENISA], 2016). Poleg tega takšni avtomobili vključujejo tudi internet stvari, ki uporabnikom (tako voznikom kot potnikom) takšnih vozil omogoča napredno rabo avtomobila z namenom izboljšanja uporabnikove izkušnje in izboljšanja varnosti avtomobilov (ENISA, 2016). Definicija, uporabljena v tem članku, je skupek več definicij (Barret, 2012; Bernik in Markelj, 2014; Chui, Löffler in Roberts 2010; ENISA, 2016; Eskandarian, 2012a; Školc, 2018) in se glasi: *Pametni avtomobili so vozila, ki so del IoT (interneta stvari) in imajo kot mobilne naprave prilagojen operacijski sistem ter dostop do interneta in drugih*

[1] Stališča, izražena v tem članku, so stališča avtorjev in jih ni mogoče pripisati Ustavnemu sodišču Republike Slovenije.

[2] Dr. Blaž Markelj, docent za varnostne vede na Fakulteti za varnostne vede Univerze v Mariboru, Slovenija. E-pošta: blaz.markelj@fvv.uni-mb.si

[3] Gašper Školc, mag. varst., Fakulteta za varnostne vede Univerze v Mariboru, Slovenija. E-pošta: gasper.skolc@student.um.si

[4] Vanja Ida Erčulj, mag. stat., predavateljica na Fakulteti za varnostne vede Univerze v Mariboru, Slovenija. E-pošta: vanja.erculj@fvv.uni-mb.si

[5] Dr. Sabina Zgaga, svetovalka na Ustavnem sodišču Republike Slovenije in docentka za kazensko pravo na Pravni fakulteti Univerze v Ljubljani, Slovenija. E-pošta: sabina.zgaga@us-rs.si

mobilnih naprav brez fizične povezave (brezžično). Prav tako gre za sisteme, ki uporabljajo računalnike, kontrole, komunikacije in avtomatizirane tehnologije za zagotavljanje varnosti na splošno, in učinkovitosti transporta z zmanjšanjem porabe energije in okoljskega vpliva.

Eskandarian (2012b) razdeli pametne avtomobile glede na stopnjo avtonomnosti, in sicer pametni avtomobili z visoko stopnjo avtonomnosti, kjer je avtomobil zmožen voziti brez pomoči voznika; s srednjo stopnjo avtonomnosti, kjer avtomobil pomaga vozniku, kolikor je to potrebno; ter s stopnjo čiste vožnje, kjer pametni avtomobil prepusti ves nadzor nad vozilom vozniku in ga zgolj opozarja na možne napake. V avtomobilu se samodejno izvajajo aktivnosti, kot je ABS sistem, sistem za stabilizacijo ter drugi sistemi in komponente, ki neprestano merijo stanje avtomobila in pomagajo pri zagotavljanju varne in udobne vožnje. S tem se zbirajo podatki o načinu upravljanja vozila in beleži voznikov personaliziran način vožnje (Školc, 2018). Schwartz (2004) pravi, da je osebni podatek pomembna valuta v 21. stoletju, saj je vrednost osebnih podatkov visoka in še vedno narašča. Zakon o varstvu osebnih podatkov (ZVOP-1, 2007) navaja, da je varstvo osebnih podatkov zagotovljeno vsakemu posamezniku ne glede na narodnost, raso, barvo, veroizpoved, etnično pripadnost itn. Prav tako definira osebni podatek kot *katerikoli podatek, ki se nanaša na posameznika, ne glede na obliko, v kateri je izražen.*

2 Arhitektura pametnega avtomobila

European Union Agency For Network And Information Security (ENISA, 2016) je oblikovala tipično oziroma splošno arhitekturo pametnih avtomobilov in sredstva znotraj le-te. Nakrani (2015) pravi, da je z napredkom tehnologije avtomobil postal prostor za medijsko rabo, kot komunikacijski center in kot delovni prostor. Prav tako se v avtomobilu s tem povečuje število uporabnih funkcij. Glede na ENISA (2016) je večina pametnih avtomobilov sestavljenih iz domen (Podomrežje prenosa moči (angl. *Power train sub-network*); Podomrežje kontrole šasije (angl. *Chassis control sub--network*); Podomrežje kontrole telesne strukture avtomobila (angl. *Body control sub-network*) in Podomrežje lahkotno prikazanih informacij (angl. *Infotainment sub-network*, v nadaljevanju: infotainment domena)), ki so med seboj povezane preko skupnega prehoda. Vse omenjene domene predstavljajo določeno tveganje za pametne avtomobile, ta tveganja se lahko razlikujejo glede vpliva na varnost in zasebnost. Osredotočili se bomo na domeno, ki lahko predstavlja najvišje tveganje, ko gre za varovanje zasebnosti. Infotainment domena (vključuje navigacijo (GPS), komunikacije (telefon ipd.) ter druge zabavne storitve (avdio/video enota – multimedijska enota)) je ločena od preostalih domen. Elektronska kontrolna enota in sistem senzorjev potnikom omogočata upravljanje mnogih funkcij, kot na primer z glavno multimedijsko enoto za avdio/video vsebino, navigacijo ter upravljanje uporabnikovega telefona. Poleg zabavnih storitev (avdio/video) ta domena ponuja še dostop do spleta, dostop do prometnih informacij, zemljevidov, digitalnega tahografa itd. (Školc, 2018). Za elektronsko kontrolno enoto v tej domeni se lahko uporabljajo operacijski sistemi mobilnih naprav, kot so Windows CE (se ne uporablja), Android, Tizen ali WebOS. Infotainment domena vključuje Bluetooth ali Wi-Fi omrežja. Enota za komunikacije skrbi predvsem za povezljivost, poleg tega pa vsebuje tudi večino varnostnih zaščit za komunikacije, kot so požarni zid, preverjanje pristnosti itd. Omenjena enota se uporablja v primerih diagnostike (obvestila o napakah, posodobitvah programske opreme itd.), obveščanje o nesreči in klic v sili, v primeru kraje avtomobila ali sporočanju položaja (geo-fencing) itn. Poleg Wi-Fi in 3G povezljivosti nudi tudi druge vmesnike, ki so namenjeni komunikaciji na dolge razdalje, in žične ter brezžične vmesnike, ki so namenjeni lokalni uporabi (ENISA, 2016).

Meola (2016) pravi, da bo v letu 2021 prodanih 82 % pametnih avtomobilov, za katere meni, da so najpomembnejši del interneta stvari v avtomobilski industriji. Poleg tega pravi, da se vedno bolj razvija integracija aplikacij v avtomobile, in sicer aplikacije za navigacijo (nadomeščajo prvotne GPS sisteme avtomobila), glasbene aplikacije (odpravljanje potrebe po radiih) ipd.

3 Varnost v pametnih avtomobilih

Čeprav se s pametnimi avtomobili soočamo zgolj zadnjih nekaj let, pa obstaja že mnogo objav glede napadov na pametne avtomobile ter avtomobilske sisteme. Omenjena problematika pa ne bi bila tako pereča, če pri tem ne bi bili ogroženi tako varnost kot tudi podatki uporabnikov takšnih vozil. Heberle, Löwe, Gustafsson in Vorrei (2017) dodajajo, da so ogrožena tako lahko tudi podjetja, katerih podatki se pretakajo preko pametnih avtomobilov. Završnik (2010) poudarja, da smo priča različnim oblikam konstantnega nadzora: prek mobilnih naprav, RFID predmetov in dokumentov ter prek sistemov za lociranje vozil. Poleg tega pravi, da so naša lokacija, komunikacija ter posledično tudi naše potrebe, želje in interesi podrobno analizirani ter smo tako (lahko) profilirani in podatkovno razkriti mnogim grožnjam. Takšne grožnje ne vplivajo zgolj na uporabnike, ampak tudi na proizvajalce, saj se zaradi izkoriščanja groženj in zaradi prisotnosti ranljivosti morajo soočati s številčnimi ponovnimi vpoklici vozil. Bernik in Meško (2011) dodajata, da je poznavanje stanja in zavedanje o ogroženosti kibernetskega prostora (znotraj katerega so tudi pametni avtomobili) nujno, če želimo zmanjšati vplive

groženj tako na posameznika kot na podjetja. Številne institucije, med njimi tudi ENISA, želijo doseči, da bi proizvajalci avtomobilov na podlagi vpeljave tako imenovanih dobrih praks dosegli varnost pametnih avtomobilov, ki bi jih ščitila pred številnimi kibernetskimi grožnjami, ki so jim nenehno izpostavljeni. Varnost oziroma zaščita pametnih avtomobilov pa je odvisna od vseh sestavnih delov in sistemov, med katere sodijo oblačne storitve, aplikacije, avtomobilske komponente, vse do vzdrževalnih in diagnostičnih orodij. Pri tem je smiselno poudariti, da kibernetska varnost pametnih avtomobilov ne vpliva zgolj na varnost in zasebnost uporabnikov takšnih vozil, ampak močno vpliva na varnost kot širši pojem. Za proizvajalce pametnih avtomobilov kibernetska varnost še vedno predstavlja največji izziv in seveda tudi strošek (ENISA, 2016).

Kot navaja ENISA (2016), so številni strokovnjaki s področja avtomobilistične industrije, natančneje s področja pametnih avtomobilov, prišli do treh kategorij dobrih praks, in sicer do politike, standardov in organizacijskih ukrepov ter varnostnih funkcij. Payne III. (2017) navaja, da avtomobil lahko vsebuje enormne količine podatkov, za kar ni nujno, da uporabnik vozila sploh ve. Ko želimo pametni telefon povezati s pametnim avtomobilom, nas sistem vedno opozori, ali želimo prenesti informacije iz telefona v sistem pametnega avtomobila. Podatki, ki se pri tem prenesejo, pa so lahko tekstovna sporočila, telefonski klici ter razne druge informacije. Poudarja, da četudi uporabnik zavrne ponudbo vozila o izmenjanju informacij, lahko vozilo še vedno zabeleži podatke o povezani napravi. Uporabnik pametnega avtomobila se ne zaveda, da lahko takšno vozilo beleži podatke celo o tem, kolikokrat so bila odprta in zaprta vrata, prižgane luči, pot, ki smo jo vnesli v navigacijski sistem, naše najljubše lokacije ter shranjene lokacije samega vozila. Pozitivni vidik hranjenja takšnih informacij je v tem, da lahko le-te pripomorejo pri preiskovanju kaznivih dejanj (na primer terorizma). Payne III. (2017) navaja tudi, da se uporabniki ne zavedajo, koliko informacij lahko hrani pametni avtomobil, zato lahko že ob pošiljanju slike vozniškega dovoljenja, kreditne kartice ali zgolj številke kreditne kartice nepooblaščena oseba, ki dostopa do teh informacij, povzroči neljubi dogodek, ki lahko pripelje celo do kraje identitete ali do finančnega oškodovanja. Peppet (2014) dodaja, da se beležijo tudi navade uporabnikov pametnih avtomobilov in vsakodnevna opravila, ki jih z njim opravljajo. Poleg tega navaja, da lahko zavarovalnice na podlagi teh podatkov ugotovijo, kako uporabnik vozi, kar bi teoretično lahko zmanjšalo stroške zavarovanja. Silberg, Plesco, Rotman in Le (2016) pa dodajajo, da pametni avtomobili zbirajo milijarde podatkov in informacij o voznikovih navadah, naklonjenostih in trenutnih podatkih o avtomobilu ter diagnostikah. To odpira nove poglede proizvajalcem avtomobilov, saj tako vedo, kaj dotični voznik potrebuje, kako se obnaša ter kako upravlja vozilo. Navedeno po eni strani omogoča proizvajalcem izboljšati varnost avtomobilov, po drugi strani pa jim omogoča prodajo (angl. *monetize*) podatkov. Avtorji nadalje navajajo, da lahko proizvajalci s pomočjo zbranih podatkov že obstoječim uporabnikom pametnih avtomobilov ne prodajajo zgolj avtomobilov, temveč tudi druge storitve, kot so »premium« parkiranje, prevoz avtomobilov, izposoja avtomobilov, polnjenje baterij, točenje goriva itn.

4 Kibernetske grožnje pametnemu avtomobilu

Uresničitev groženj, ki jih navaja ENISA (2016), so »izhodišče« za uresničitev kibernetske kriminalitete znotraj interneta stvari in pametnih avtomobilov.

Grožnje, ki jih lahko nepooblaščene osebe uresničijo, so (ENISA, 2016):

— škoda/izguba (izguba informacij v oblaku, izguba/uhajanje občutljivih informacij – informacije o plačilu, vozniških navadah idr. pri prodaji vozila drugemu lastniku …),

— *prisluškovanje/prestrezanje/ugrabitev* (ponovitev sporočil, brez ustrezne zaščite lahko napadalci bolj preprosto upravljajo zaviranje, krmiljenje idr. funkcije avtomobila),

— MITM (angl. *man in the middle*) oz. ugrabitev seje (možna je finančna izguba, nalaganje škodljive programske opreme, pridobitev zakonitega ključa, s katerim se avtomobil odtuji, omrežno zbiranje informacij …),

— *kriminalna dejanja/zloraba* (onemogočanje storitve (DoS, DDoS) – ne zgolj izpad omrežja, ampak tudi nepričakovano vedenje vozila; nepooblaščen dostop do informacijskega sistema/omrežja (napadalci prevzamejo nadzor nad vozilom));

— *razkritje zaupnih informacij*,

— *identitetna prevara* (največkrat gre za kloniranje ključa z namenom napačnega predstavljanja avtomobila sistemom cestne infrastrukture (plačilo cestnine ipd.)) in

— *zlonamerna programska oprema/dejavnost* (izkoriščanje znanih poti napadov na Linux, Android in Windows okolja. Ti napadi se s časom izvajajo tudi nad pametnimi avtomobili.). Završnik in Sedej (2012) med kibernetske grožnje štejeta tudi nadlegovanje, kar se lahko dogaja tudi pri rabi pametnega avtomobila in je lahko povezano z drugimi napadi, opisanimi zgoraj. Browne (2016) navaja, da večina ljudi ne kaže pomislekov glede kibernetske varnosti pri uporabi pametnih avtomobilov ter naprav interneta stvari. Problematika se pojavi v dejstvu, da potrošniki želijo vedno večjo povezljivost naprav z zunanjim svetom, s katere koli lokacije, kar pa privede do morebitnih ranljivosti sistemov in s tem posledično uporabnikove zasebnosti. Ob tem dejstvu ne smemo pomisliti zgolj na pametne avtomobile, ki se

lahko povezujejo s hišnim varnostnim sistemom, pametnimi televizijami, pametnimi hladilniki ter drugimi pametnimi napravami, ampak tudi na pametne domove ter stanovanja in na osebne podatke, ki jih te naprave hranijo. Vse te naprave so povezane preko številnih omrežij, ljudje pa se pri vsem tem ne zavedajo vedno ranljivosti takšnih sistemov. Ljudje se še vedno bolj zavedajo glede varnosti in varnostnih ranljivosti osebnih računalnikov kot pa iste problematike pri mobilnih napravah, med katere lahko štejemo tudi pametne avtomobile ter naprave interneta stvari.

Današnji avtomobili uporabljajo na stotine senzorjev, ki se povezujejo z mnogimi med seboj povezanimi računalniki, vsa ta tehnologija pa ne zagotavlja uporabniku zgolj udobja med potovanjem, ampak tudi varnost. Hartfield (2017) pravi, da integracija pametnih telefonov v avtomobile ni posledica nenehnega pritiskanja ponudnikov IT storitev, ampak tudi posledica proizvajalcev avtomobilov samih, kar se kaže tudi pri oblikovanju lastne tehnologije, kot je na primer BMW-jev Connected Drive, Volkswagnov Car-Net, Mercedesov mbrace itd. Med številne ranljive sisteme Hartfield (2017) uvršča tudi: USB, ki povečuje možna tveganja za napade na pametne avtomobile (USB sicer omogoča povezovanje naprav za predvajanje glasbe, za navigacijo ali za polnjenje naprav, vendar je lahko le-ta vmesnik velikokrat tarča napadalcev, ki lahko spremenijo strojno programsko opremo USB (česar končni uporabnik ne more zaznati), napadalci pa lahko s tem spreminjajo nastavitve vozila); Bluetooth, ki se največkrat uporablja za namene prenašanja imenikov oziroma stikov v sistem avtomobila, prenašajo pa se lahko še gesla in aplikacije, ki jih napadalci lahko izkoristijo z namenom prisluškovanja, kraje osebnih podatkov ali drugih zlonamernih dejanj. Z integracijo pametnih telefonov v pametne avtomobile prinesemo še dodatne ranljivosti, ki tičijo v komunikacijskih kanalih, kot so 3G/4G, Wi-Fi, Bluetooth itd. Poleg tega so lahko zelo problematične tudi aplikacije tretjih oseb, ki jih uporabniki prenašajo na svoje pametne telefone. Takšnim aplikacijam dodelimo določene privilegije, ki lahko ogrožajo lastnika. Med mobilnimi platformami, ki se najpogosteje soočajo s to problematiko, sta Apple iOS ter Android (Harfield, 2017).

McAfee (2017) navaja, da je vsaka elektronska naprava sestavljena iz več komponent, ki so proizvedene s strani mnogih proizvajalcev/dobaviteljev. Strojna oprema, programska oprema, razvijalna orodja, testna orodja in še mnoga druga niso produkt enega proizvajalca. Problematika takšne proizvodnje se pojavi pri tem, da so takšni izdelki običajno cenejši in potrošnikom dostopnejši. Takšen proces proizvodnje privede do varnostnih tveganj, saj proizvajalci takšnih komponent ne nujno uporabljajo enake stopnje varnosti, kot jih proizvajalci originalnih delov. To je lahko tudi velik problem ekološkega onesnaževanja z elektronskimi odpadki. Cenejši deli se namreč velikokrat hitro tudi uničijo in zavržejo na nepravilen način (Eman in Franca, 2016). Mcafee (2017) prav tako navaja, da je treba odkrivati takšne komponente in zagotavljati varnostne ukrepe pri dobavni verigi: uporaba pooblaščenih distribucijskih kanalov za nabavo strojne in programske opreme za vzdrževanje ter sestavo avtomobilov; uporaba sledenja, ki zaznava kritične komponente, ki vključujejo varnostne sisteme; neprekinjenost oskrbe, ki vključuje dolgoročno politiko razpoložljivih nadomestnih delov; beleženje tveganj, ki nastanejo v proizvodnih procesih; nadzor končnih izdelkov z možnimi tveganji (napačen opis, ponarejanje itd.). Poleg fizičnih ustavitev avtomobilov, upravljanja klimatske naprave, ventilatorjev in brisalcev pa lahko napadalci svoje napade usmerjajo tudi drugam, kot so: kraja avtomobila ali elektronska škoda/onemogočanje delovanja; poneverba podatkov o vozilu (število prevoženih kilometrov); dostop do osebnih podatkov (mobilne številke, naslovi, bančni podatki, lokacija itd.) za takojšnjo uporabo ali izsiljevanje; prisluškovanje zvočni in podatkovni komunikaciji uporabnika in avtomobila; ter dostop do proizvajalca periferij, ponudnika storitev ali do podatkov o prodajalcu aplikacij oz. aplikacijah samih (Schorer, 2015). Georgiadis, Polatidis, Mouratidis in Pimenidis (2017) dodajajo, da tako pridobljeni podatki lahko služijo tudi kot »nadležno« vsiljevanje personaliziranih reklam v avtomobilu. Na podlagi resničnih primerov vidimo, da je informacijska varnost znotraj pametnih avtomobilov še vedno v razvoju.

4.1 Primeri uresničitve kibernetske kriminalitete v pametnih avtomobilih

V nadaljevanju navajamo nekatere primere, v katerih so storilci izkoristili informacijskovarnostne pomanjkljivosti pametnih avtomobilov in izvedli napad na njihov informacijski sistem.

Prvi primer je iz leta 2017, ko je Smith (2017) poročal o incidentu, ki naj bi se zgodil v Londonu. Neznanca sta s pomočjo naprave, ki jo je mogoče kupiti preko spletne trgovine *eBay,* povečala doseg ključa (ki je bil v hiši žrtve) novega avtomobila BMW, ga tako odklenila in s pomočjo te naprave tudi prižgala ter odpeljala. Ta primer kaže na še vedno veliko ranljivost brezstičnih ključev tudi v avtomobilih, ki so višjega cenovnega razreda.

V drugem primeru Greenberg (2016) prikaže, kako sta raziskovalca Charlie Miller in Chris Valasek v Angliji oddaljeno zavzela določene kontrole vozila znamke Jeep Cherokee podjetja Chrysler. Napad sta prvič izvedla v letu 2015 preko enote, ki se fizično poveže z računalnikom, in vdrla v elektronsko krmilno enoto ter si tako odprla vrata do nekaterih delov avtomobila, ki so jima preko oddaljenih ukazov poma-

gali upravljati določene elemente (npr. vklop brisalcev, izklop zavor pod 8 km/h, obračanje volana, ko je bila prestavna ročica v vzvratni legi ipd.). Po tem napadu je Chrysler vpoklical 1,4 milijona svojih vozil, da bi namestil posodobitve, ki bi tak napad onemogočile. Leto kasneje sta Miller in Valasek z novo tehniko vdrla v omrežje krmilnika enakega avtomobila, ki jima je pomagala zaobiti določena varovala, ki so jima v prvem poskusu onemogočala izvajanje napadov v celoti. Preko dostopa do omrežja krmilnika sta z oddaljene lokacije avtomobilu pošiljala ukaze, s katerimi sta lahko nadzorovala celotno vozilo (med drugim tudi hitro zaviranje, zmanjšanje hitrosti, obračanje volana med vožnjo ipd.). Školc (2018) pravi, da je ta primer pokazal, da so pametni avtomobili enako ranljivi, kot so ranljivi osebni računalniki ali druge mobilne naprave, vendar se napadi na njih lahko izkažejo za bolj ogrožajoče, saj niso ogroženi zgolj podatki voznikov, ki se z avtomobili povezujejo, temveč tudi njihovo zdravje.

Tretji primer nam pokaže, da se kljub dobri zaščiti uporabnikovi podatki v vozilu hranijo nešifrirani. Constantin (2017) navaja, da je možno skozi USB vhod prenesti škodljive skripte, ki jih sistem samodejno zažene s polnimi administrativnimi pravicami. To je ugotovil Gabriel Cîrlig (v Constantin, 2017), poleg tega pa je v infotainment modulu našel nešifrirane podatke uporabnikov povezanih mobilnih naprav (npr. zgodovina klicev, tekstovna in elektronska sporočila, imeniki itd.). Poleg teh podatkov je našel tudi druge občutljive podatke, kot je seznam priljubljenih lokacij, s katerih oz. proti katerim je avtomobil potoval; zvočni profili ukazov; ter GPS koordinate, ki jih je uporabnik vnašal v GPS enoto infotainment modula. Vsaka zaščita mobilnih naprav je tako nepredmetna, saj se preko Bluetooth povezave združi z infotainment domeno v takem pametnem avtomobilu, kot ga je preiskoval Cîrlig. Prav tako pravi, da je infotainment modul tega avtomobila japonske izdelave paradiž za hekerje, saj uporablja WiFi ter GPS, osnovan je na operacijskem sistemu Linux, s polnim dostopom do terminala, prav tako pa naj bi v tem modulu ostala mnoga orodja za odkrivanje napak (tudi za GPS sistem), ki jih razvijalci niso izbrisali. Obstaja še en primer možnih groženj, ki pretijo uporabnikom pametnih avtomobilov. Vozniki so namreč tisti, ki so poleg nezaščitenih podatkov največji problem, saj lahko z zlonamernim USB ključem napadalci pridejo do njegovih podatkov, poleg tega pa mu lahko neprestano išče odprta WiFi omrežja in dostopa do podatkov o lokaciji v živo.

5 Kazniva dejanja, povezana z motornimi vozili, v Sloveniji in drugih evropskih državah

Ker števila vseh kaznivih dejanj, povezanih z motornimi vozili, nismo našli, smo se osredotočili na kazniva dejanja, povezana s tatvinami motornih vozil. Kolenc, Kebe in Bukovnik (2014) navajajo, da je bilo v letu 2013 kaznivih dejanj, povezanih s tatvinami motornih vozili, več kot v letu 2012 (tabela 1). Japelj (2015) dodaja, da je bilo v letu 2014 teh kaznivih dejanj 782, kar je 6,1 % manj kot v letu 2013. V letu 2015 pa je bilo kaznivih dejanj, povezanih z motornimi vozili, 569, kar je 27,2 % manj kot leto prej. Japelj (2016) pravi, da je trend napadov na informacijske sisteme pozitiven, kar pomeni, da se bodo povečevali tudi napadi na pametne avtomobile. Poleg tega pravi, da se lahko glede na tehnološki razvoj upravičeno pričakuje povečanje števila tovrstnih kaznivih dejanj na dolgi rok. S takimi kaznivimi dejanji si storilci lahko pridobijo tudi premoženjsko korist (npr. s tatvino denarnih sredstev po sistemu e-bančništva, telefonije in drugih sistemov ter povezav, ki jih pametni avtomobili omogočajo) (Kolenc, Kebe in Bukovnik, 2013).

Tabela 1: Tatvine motornega vozila med letoma 2004 in 2013 (vir: Kolenc, Kebe in Bukovnik, 2014)

Leto	Št. tatvin motornih vozil
2004	704
2005	873
2006	852
2007	839
2008	582
2009	584
2010	529
2011	522
2012	528
2013	618

Slovenija še zdaleč ni osamljena država, v kateri se izvajajo kazniva dejanja, povezana z avtomobili. Mijalković, Bošković, Vuković in Vučković (2016) navajajo, da je bilo v Republiki Srbiji med letoma 1994 in 2013 zabeleženih 84.887 tatvin vozil, kar je povprečno 4.244 vozil na leto, najpogostejše (92,1 % vseh) so bile tatvine osebnih avtomobilov. Dodajajo, da je bila za krajo vozil uporabljena sodobna tehnologija in hitro obvladovanje najnovejših sredstev za zavarovanje vozil proti krajam. Poleg tega naj bi tatovi uporabljali elektronske naprave ter prilagojeno programsko opremo za nevtralizacijo osrednjega računalnika vozila ter izdelali posebne ključe za vžig motorja. Mijalković et al. (2016) navajajo tudi, da se je med letoma 2002 in 2011 trend tatvin avtomobilov povečal v Albaniji (za 267 %), na Cipru (215 %), Bolgariji (52 %) ter Rusiji (6 %). Navajajo, da se je v drugih evropskih državah ta trend zmanjšal, in sicer največ v Veliki Britaniji, kjer se je zmanjšal za 70 %, ter v Španiji, Belgiji in na Poljskem, kjer se

je zmanjšal za 10 % manj kot v Veliki Britaniji. Za isto obdobje je imela Švedska najvišjo stopnjo tatvin motornih vozil, in sicer 567 na 100.000 prebivalcev. V državah Evropske unije se je stopnja tatvin zmanjševala povprečno za 15,72 vozil na leto. Kar pa, tudi ob upoštevanju zgoraj navedenih ugotovitev iz Slovenije (Japelj, 2015, 2016; Kolenc et al., 2013, 2014), kaže na to, da se ti trendi po letu 2011 ponovno spreminjajo na pozitivne, predvsem zaradi vstopa avtomobilov v kibernetski svet in s tem večjega tveganja za uresničitev groženj tudi zoper pametne avtomobile.

6 Statistični podatki napadov na informacijske sisteme

Glede na to, da postajajo pametni avtomobili vse bolj pogosto del interneta stvari (IoT), lahko rečemo, da so grožnje, ki pretijo drugim IoT napravam, vedno bolj usmerjene tudi proti njim. Symantec (2017) je v svojem letnem poročilu internetnih groženj (»*Internet Security Threat Report*«) zabeležil 7,1 milijardo razkritih identitet preko vdorov v informacijske sisteme v zadnjih osmih letih. S pametnimi avtomobili se lahko povezujemo tudi v internet in pregledujemo elektronsko pošto, zato je smiselno, da omenimo, da je trend groženj glede na Symantecovo poročilo v porastu. Leta 2015 je bilo namreč 53 % elektronske pošte neželene oz. spam pošte, od tega phishing napadov eden na 1.846 sporočil in škodljive programske opreme ena na 220 sporočil. V letu 2016 se trend neželene pošte ni spremenil količinsko, vendar je bilo manj phishing napadov (zgolj eden na 2.596 sporočil) ter več škodljive programske opreme (ena na 131 sporočil). Na podlagi teh podatkov lahko rečemo, da je škodljiva programska oprema v porastu in lahko pričakujemo, da se bo to število še povečevalo tudi v pametnih avtomobilih. Kar je še vedno težava, saj ljudje še vedno nasedajo »nigerijskim prevaram« v e-pošti (Lamberger, Slak in Dobovšek, 2013). Symantec (2017) je prav tako preveril napade na mobilne naprave (mobiteli, tablični računalniki ipd.), ki se vedno bolj povezujejo s pametnimi avtomobili. V zadnjih nekaj letih se je povečalo število izsiljevalskih virusov; v letu 2015 so zabeležili 340.665 napadov na mobilne naprave s povprečno vsoto odkupnine 294 dolarjev, v letu 2016 pa 463.841 napadov s povprečno vsoto odkupnine 1.077 dolarjev. Pravijo, da je več takih napadov na Android platformah, vendar ne izključujejo možnosti, da bodo napadi na iOS platforme ostali v nizkih številkah. Kar pomeni, da se tovrstni napadi lahko v prihodnosti uresničijo vedno bolj pogosto tudi v pametnih avtomobilih, vendar s hujšimi posledicami (Školc, 2018). Zelo pomemben podatek, ki ga je Symantec (2017) v svojem poročilu izdal, je, da sta za napad na IoT naprave potrebni zgolj dve minuti. Nova IoT naprava, povezana v internet (s tem tudi pametni avtomobili), je tako lahko v dveh minutah po priklopu v internet del BotNeta[6] brez vednosti uporabnika.

Tudi ENISA (2017) poroča, da je v letih od 2009 do 2017 prišlo do porasti napadov na IoT naprave. Med drugim je v letu 2015 raziskovalcem uspelo priti do fizičnega dostopa v pametne avtomobile znamke BMW, preko njihovih strežnikov z oddaljenim dostopom. Vse pogosteje pa omenjajo tudi DDoS napade od leta 2016, kar nakazuje na porast tovrstnih groženj in s tem pozivajo k boljšemu varovanju IoT naprav, med drugim tudi pametnih avtomobilov.

7 Kazenskopravni vidik uresničitve nekaterih groženj pametnim avtomobilom

Uresničitev groženj pametnim avtomobilom, ki so zgoraj predstavljene po sistematizaciji, ki jo je napravila ENISA, lahko pomeni tudi izpolnitev zakonskih znakov kaznivega dejanja ali vsaj prekrška. Le-to je lahko naperjeno zoper voznika pametnega avtomobila, lahko pa tudi zoper tretjo osebo, ki je kot potnik bodisi v pametnem avtomobilu bodisi izven pametnega avtomobila. Glede na zgoraj predstavljene grožnje bodo tako v nadaljevanju predstavljeni nekateri kazenskopravni poudarki, zlasti pa dileme in normativni problemi, ki se pojavljajo ob uresničevanju groženj pametnim avtomobilom.

Kot prvo grožnjo ENISA navaja izgubo podatkov, tudi občutljivih, ki se zbirajo ob upravljanju pametnega avtomobila. Podatki o lokaciji, kjer se je vozil pametni avtomobil, kdo ga je vozil, način plačila itd., so osebni podatki po Zakonu o varstvu osebnih podatkov (2007). Do izgube osebnih podatkov lahko v povezavi s pametnimi avtomobili pride bodisi tako, da zakoniti upravljavec osebnih podatkov podatke posreduje neupravičeni osebi, bodisi s tem, da tretja oseba neodvisno od tega pridobi te podatke. Naklepno posredovanje osebnih podatkov brez pravne podlage je lahko prekršek po prvi točki prvega odstavka 91. člena ZVOP-1 (2007).[7] Za kaznivo deja-

[6] BotNet je zbirka naprav, povezanih v internet (računalniki, mobilne naprave, IoT naprave itd.), ki so okužene in upravljane z enako škodljivo programsko opremo. Take naprave kibernetski kriminalci uporabljajo predvsem za pošiljanje neželene pošte in ustvarjanje škodljivega prometa (DDoS napadi oz. napadi za distribuirano zanikanje storitev) (Rouse in Wright, 2017).

[7] 91. člen ZVOP-1 (2004) določa: »(1) Z globo od 4.170 do 12.510 evrov se kaznuje za prekršek pravna oseba, samostojni podjetnik posameznik ali posameznik, ki samostojno opravlja dejavnost: 1. če obdeluje osebne podatke, ne da bi imel za to podlago v zakonu ali v osebni privolitvi posameznika (8. člen).« Tretja točka prvega odstavka 6. člena ZVOP-1 pa določa: »Obdelava osebnih podatkov – pomeni kakršnokoli delovanje ali niz delovanj, ki se izvaja

nje zlorabe osebnih podatkov po 143. členu Kazenskega zakonika – 1 (KZ-1, 2012, 2015, 2016) gre namreč le v primeru, če se ti podatki posredujejo v javno objavo ali jih javno objavi.[8] Če pa so izpolnjeni pogoji pomoči, zlasti, da se upravljavec osebnih podatkov, zbranih v zvezi z upravljanjem pametnega avtomobila, zaveda, da bo tretja oseba te podatke uporabila za izvršitev drugega kaznivega dejanja, in da to hoče (t. i. dvojni naklep pomagača), pa lahko upravljavec osebnih podatkov odgovarja za pomoč pri tem drugem kaznivem dejanju.

Tretja oseba lahko pridobi podatke o upravljanju pametnega avtomobila tudi brez naklepnega prispevka upravljavca osebnih podatkov. Če je upravljavcu osebnih podatkov, pridobljenih iz pametnega avtomobila, mogoče očitati malomarnost za opustitev ustreznih ukrepov za zaščito teh podatkov, prihaja še vedno v poštev odgovornost vsaj za prekršek po 93. členu ZVOP-1 (2007), tj. za kršitev določb o zavarovanju osebnih podatkov oziroma za opustitev potrebnega zavarovanja osebnih podatkov.[9] Kaznivega dejanja iz 143. člena KZ-1 (2012, 2015, 2016) pa za razliko od omenjenega prekrška ni mogoče izvesti iz malomarnosti, ampak zgolj z naklepom.

Tretja oseba lahko za nepooblaščen dostop do osebnih podatkov, pridobljenih pri upravljanju pametnega avtomobila, odgovarja tudi po drugem odstavku 143. člena KZ-1 (2012, 2015, 2016), in sicer, če vdre ali nepooblaščeno vstopi v računalniško vodeno zbirko podatkov z namenom, da bi sebi ali komu drugemu pridobila osebni podatek. Glede na to, da je poseben način izvršitve oziroma pridobitve osebnih podatkov predviden kot zakonski znak po drugem odstavku 143. člena KZ-1 (2012, 2015, 2016), pravi stek kaznivega dejanja po drugem odstavku 143. člena KZ-1 (2012, 2015, 2016) s kaznivim dejanjem iz 221. člena KZ-1 (2012, 2015, 2016, napad na informacijski sistem) v primeru izvršitvenega ravnanja vdora ali nepooblaščenega vstopa z namenom pridobitve osebnega podatka praviloma ne pride v poštev. Pravi stek bi bil mogoč le, če bi bili ti podatki pridobljeni z drugimi izvršitvenimi ravnanji, kot tistimi, opredeljenimi v 221. členu KZ-1 (2012, 2015, 2016).

ENISA kot možno grožnjo pametnim avtomobilom izpostavlja tudi prevzem nadzora nad pametnim avtomobilom v celoti oziroma nad delom njegovega sistema oziroma operacijskega sistema. Če popoln prevzem nadzora nad pametnim avtomobilom pomeni, da voznik in potniki ne morejo zapustiti vozila, je lahko v takem primeru storjeno tudi kaznivo dejanje protipravnega odvzema prostosti iz 133. člena KZ-1 (2012, 2015, 2016),[10] ob obstoju posebnega namena prisiljenja k storitvi, opustitvi ali trpljenju za to pa tudi kaznivo dejanje ugrabitve iz 134. člena KZ-1 (2012, 2015, 2016). Bistveno za dokončanje tega kaznivega dejanja je, da je podana protipravna omejitev svobode gibanja. Glede na tehnične lastnosti pametnega avtomobila je tudi ti kaznivi dejanji praviloma mogoče izvesti z napadom na informacijski sistem (221. člen KZ-1, 2012, 2015, 2016), zato se spet odpira vprašanje stekov s tem kaznivim dejanjem in kaznivim dejanjem iz drugega odstavka 143. člena KZ-1 (2012, 2015, 2016). Glede na različne pravne dobrine, varovane s kaznivimi dejanji, in *lex specialis* naravo kaznivega dejanja iz drugega odstavka 143. člena KZ-1 (2012, 2015, 2016) v primerjavi s kaznivim dejanjem iz 221. člena KZ-1 (2012, 2015, 2016) prihaja praviloma v poštev pravi stek med kaznivim dejanjem iz 133. oziroma 134. člena KZ-1 (2012, 2015, 2016) in drugega odstavka 143. člena KZ-1 (2012, 2015, 2016).

Vprašanje pa je, kaj bi pomenil prevzem zgolj dela operacijskega sistema pametnega avtomobila, ne da bi bila osebam v njem onemogočena svoboda gibanja. Praviloma v takem primeru ne bi prišlo v poštev le kaznivo dejanje po drugem odstavku 143. člena KZ-1 (2012, 2015, 2016, nepooblaščen vstop ali vdor z namenom pridobiti osebni podatek), ampak tudi kaznivo dejanje po 221. členu KZ-1 (2012, 2015, 2016), zlasti izvršitveno ravnanje po drugem odstavku 221. člena KZ-1 (2012, 2015, 2016), tj. oviranje delovanja informacijskega sistema. Če je z dejanjem iz drugega odstavka tega člena povzročena velika škoda, je relevantna tudi kvalificirana oblika kaznivega dejanja po četrtem odstavku 221. člena KZ-1 (2012, 2015, 2016).

v zvezi z osebnimi podatki, ki so avtomatizirano obdelani ali ki so pri ročni obdelavi del zbirke osebnih podatkov ali so namenjeni vključitvi v zbirko osebnih podatkov, zlasti zbiranje, pridobivanje, vpis, urejanje, shranjevanje, prilagajanje ali spreminjanje, priklicanje, vpogled, uporaba, razkritje s prenosom, sporočanje, širjenje ali drugo dajanje na razpolago, razvrstitev ali povezovanje, blokiranje, anonimiziranje, izbris ali uničenje; obdelava je lahko ročna ali avtomatizirana (sredstva obdelave).«

[8] Glej prvi odstavek 143. člena KZ-1 (2012).

[9] Gl. 93. člen ZVOP-1 (2007): »(1) Z globo od 4.170 do 12.510 evrov se kaznuje za prekršek pravna oseba, samostojni podjetnik posameznik ali posameznik, ki samostojno opravlja dejavnost, če v skladu s tem zakonom obdeluje osebne podatke in ne zagotovi zavarovanja osebnih podatkov (24. in 25. člen). (2) Z globo od 830 do 1.250 evrov se kaznuje za prekršek iz prejšnjega odstavka tudi odgovorna oseba pravne osebe, samostojnega podjetnika posameznika ali posameznika, ki samostojno opravlja dejavnost. (3) Z globo od 830 do 1.250 evrov se kaznuje za prekršek odgovorna oseba državnega organa ali organa samoupravne lokalne skupnosti, ki stori dejanje iz prvega odstavka tega člena. (4) Z globo od 200 do 830 evrov se kaznuje za prekršek posameznik, ki stori dejanje iz prvega odstavka tega člena.«

[10] »Kdor koga protipravno zapre, ima zaprtega ali mu kako drugače omeji svobodo gibanja, se kaznuje z zaporom do enega leta.« (KZ-1, 2012, 2015, 2016)

Kot izhaja iz predstavljenih statističnih podatkov, je relevantno kaznivo dejanje, in sicer tako pri klasičnih kot tudi pri pametnih avtomobilih, tudi tatvina pametnega avtomobila. Glede na to, da je za odvzem avtomobila običajno potreben vlom, vdor ali drugačno premagovanje večjih ovir,[11] je običajno upoštevna kvalifikacija vlomne in ne le navadne tatvine. Tudi pri tem kaznivem dejanju pa je treba upoštevati, da je za izvršitev pri pametnem avtomobilu potreben vstop v informacijski sistem pametnega avtomobila, zato je relevantno vprašanje stekov s kaznivim dejanjem iz 221. člena KZ-1 (2012, 2015, 2016). Menimo, da je treba upoštevati enako pravilo kot pri pravilih za stek med vlomno tatvino in poškodovanjem tuje stvari oziroma kršitve nedotakljivosti stanovanja, ki sta jih razvili sodna praksa in teorija. Tako bi šlo za navidezni stek, če se napad na informacijski sistem izvede zgolj zaradi vloma v avtomobil. Kar presega nujnost vdora za vlom v pametni avtomobil, pomeni pravi stek med kaznivima dejanjema.

ENISA kot upoštevno grožnjo pametnim avtomobilom določa tudi prisluškovanje sporočilom oziroma pogovorom v avtomobilu. Za to je upoštevno kaznivo dejanje neupravičenega prisluškovanja in zvočnega snemanja iz 137. člena KZ-1 (2012, 2015, 2016).

Omeniti je treba tudi situacijo, ki se verjetno zdi vsakemu vozniku pametnega vozila najbolj grozljiva, tj. prevzem nadzora nad pametnim avtomobilom z napadom na njegov informacijski sistem[12] ter povzročitev škode tretjim osebam, na primer prometne nesreče (na primer kaznivo dejanje iz 323. člena KZ-1, 2012, 2015, 2016). V takem primeru se seveda najprej pojavi vprašanje odgovornosti voznika pametnega avtomobila. Če voznik nima nobene tehnične možnosti obvladati pametni avtomobil, bi bil lahko upošteven institut absolutne sile,[13] ki izključi voljnost ravnanja in s tem kaznivo dejanje voznika pametnega avtomobila. Upoštevna pa je tudi odgovornost osebe, ki prevzame nadzor nad pametnim avtomobilom, in sicer za škodo, ki s tem nastane tretjim osebam, zlasti za naklepno (na primer telesne poškodbe ali uboj) kaznivo dejanje v obliki posrednega storilstva.

8 Zavarovanje pred kibernetsko kriminaliteto

Glede na to, da številni pametni avtomobili uporabljajo infotainment domeno, so proizvajalci vozil prisiljeni k uporabi raznovrstnih varnostnih zaščit (Školc, 2018). Te zajemajo unikatne identifikacijske številke in specifične komplete radio-frekvenčnih signalov, šifriranje, maskiranje, skeniranje, odkrivanje anomalij, uporaba certifikatov, filtriranje, uporaba požarnih zidov, sistemi za zaznavanje vdorov, uporaba bele liste, odkrivanje goljufij, šifriranje podatkov o omrežnih povezavah in zaščita ključev ter uporaba zaprtih sistemov, kjer ni omogočeno pisanje kode brez pooblaščenih orodij (Browne, 2016). National Highway Traffic Administration (NHTSA) je poskušala s pripravo Zakona o varnosti in zasebnosti v avtomobilu (Security and Privacy in Your Car Act, 2015) doseči kibernetsko varnost v avtomobilih. Doseči so želeli ustrezno zaščito pred nepooblaščenim dostopom do elektronskih kontrol ali kakršnih koli podatkov o vožnji, ki vključujejo podatke o lokaciji, hitrost, podatke o lastniku ali potnikih, prav tako pa želijo preprečiti nepooblaščen dostop do podatkov, ki jih zbirajo in shranjujejo elektronski sistemi, vgrajeni v vozilo (Pearson, 2017). Tako kot vse druge pametne naprave, bodisi pametni telefoni ali pa pametni robotski sesalniki, občasno potrebujejo nadgradnjo programske opreme, pri vsem tem pametni avtomobili niso nikakršna izjema. Anderson, Kalra, Stanley, Sorensen, Samaras in Oluwatola (2014) poudarjajo, da so lahko takšna vozila povezana med seboj, z infrastrukturo ali internetom, kar pomeni da so lahko izpostavljena kibernetskim napadom. Zaradi vse boljše povezljivosti pametnega avtomobila (internet, USB priključek, mobilni telefoni itd.) se pojavljajo novi varnostni izzivi in s tem tudi vse večje število vstopnih točk za zlonamerno izkoriščanje avtomobila ter zasebnosti uporabnika. Zavedati se je treba tudi, da je za nadgradnje programske opreme vedno potreben dostop do spleta, kar prinaša možnost, da računalniški virusi okužijo sistem pri popolnoma zakoniti nadgradnji programske opreme in tako odtujijo marsikateri osebni podatek uporabnikov. V takšnih primerih avtorji navajajo, da je treba zagotoviti izredno varne povezave s strežniki. Izmed vseh groženj, ki pretijo pametnim avtomobilom, pa nikakor ne smemo spregledati najpomembnejše grožnje, človeka. Tehnološki navdušenci vedno želijo dostopati do raznih sistemov za pridobitev nadzora nad elementi, do katerih avtomobilistični proizvajalci onemogočijo dostop. Pri mobilnih telefonih se soočamo z izrazoma »jail breaking« in »rooting«, s katerima tehnološki navdušenci pridobijo večji dostop in prilagodljivost svoje naprave. Tudi pametni avtomobili bodo lahko žrtve tega, saj si bodo uporabniki želeli boljše učinkovitosti ali uporabo svoje lastne programske opreme, pa četudi pri tem tvegajo svojo fizično varnost in varnost svojih osebnih podatkov (Anderson et al., 2014).

Preprečevanje kibernetskih napadov na pametne avtomobile Schober (2016) primerja s preprečevanjem kibernetskih napadov na osebne računalnike: Uporabniki morajo poskrbeti, da je njihova programska in strojna oprema posodobljena; Izogibajo naj se nameščanju naprav ali aplikacij, ki jih proizvajalec ni odobril; Pozorni naj bodo na nepooblaščeno

[11] Gl. prvo točko prvega odstavka 205. člena KZ-1 (2012, 2015, 2016).

[12] Kaznivo dejanje iz 221. člena (KZ-1, 2012, 2015, 2016).

[13] Za opredelitev in pomen absolutne sile glej Bavcon, Šelih, Ambrož, Filipčič in Korošec (2013: 160).

poseganje v avtomobil, saj veliko vdorov v pametne avtomobile zahteva fizičen dostop (priklop USB ključka ipd.). Ward (2017) navaja, da je potrebno zagotavljanje varnosti skozi celoten življenjski cikel avtomobilov in sistemov, ki jih uporabljajo. Beltov (2016) navaja, da vključevanje IoT v vozila ter uporaba platform pametnih avtomobilov ponuja zmožnost ogleda, nadzora ter prilagajanja nastavitev vozila preko pametnih telefonov, tabličnih računalnikov in računalnikov. Problem se pojavlja pri uporabi programov tretjih oseb za takšno manipulacijo, saj to lahko predstavlja grožnjo uporabnikovim osebnim podatkom. Zurkus (2015) pravi, da so pametni avtomobili tehnološko napredne in računalniško podprte naprave, ki so povezane z navigacijskimi ter zabavnimi sistemi. Pri vsem tem pa shranjujejo osebne podatke, ki so lahko cilj mnogih napadalcev. Problem se pojavi pri vprašanju, kdo je lastnik teh informacij, kam in na kakšen način se delijo/pošiljajo in kako proizvajalci takšnih avtomobilov ščitijo te podatke (Zurkus, 2015). Z nastopom evropske Uredbe o varstvu osebnih podatkov so ta vprašanja postala regulirana. Ko govorimo o zasebnosti v pametnih avtomobilih, je zelo smiselno, da si postavimo vprašanje, kakšne informacije sploh poseduje naš pametni avtomobil. Payne III. (2017) pravi, da bodo proizvajalci pametnih avtomobilov nedvomno začeli uporabljati skrivanje informacije, vendar, kakšen način bodo izbrali, da bodo to dosegli, je le vprašanje časa.

Za uspešno varovanje podatkov in življenj uporabnikov pametnih avtomobilov ter podatkov podjetij, v katerih delajo, so potrebne spremembe. ENISA (2017) poudarja, da je poleg klasičnih varnostnih ukrepov (sprememba privzetih gesel v zapletena gesla, šifriranje podatkov in prometa itd.) za organizacije potrebna dobro zapisana informacijskovarnostna politika, ki bo poleg splošnih varnostnih ukrepov govorila tudi o konkretnih primerih, ki so od organizacije do organizacije drugačni, in mora biti razumljiva vsem, ki jo bodo uporabljali, ter bo jasno ločila zasebno in poslovno rabo pametnih avtomobilov ter drugih IoT naprav. Organizacija mora biti seznanjena s primeri dobre prakse tudi v tehničnih elementih in jih mora sama tudi uporabljati, za čim boljše zmanjševanje tveganj napadov na pametne avtomobile (Školc, 2018).

Prav tako so pri ENISA (2017) našteli tehnične ukrepe za zagotavljanje boljše varnosti v IoT napravah (tudi v pametnih avtomobilih): *varnost strojne opreme* (uporaba dodatne strojne opreme za zviševanje stopnje varnosti, npr. posebni varnostni čipi ipd.), *menedžment zaupanja in integritete* za uporabljene naprave, *močna privzeta varnost in zasebnost* (vse neuporabljene funkcije oz. nevarne funkcionalnosti naj bodo privzeto izklopljene), *varovanje podatkov in strinjanje* (tu gre predvsem za skladnost z zakonodajo o varovanju osebnih podatkov in minimalnim zbiranjem osebnih podatkov), *varnost sistemov in njihova zanesljivost* (mehanizmi za samodejno preverjanje in odpravljanje napak), *varno posodabljanje programske opreme in sistemskih programov* (zagotovitev, da so vse posodobitve možne preko interneta, da so strežniki za posodobitve kot sama povezava varni, da se ne prenašajo občutljivi podatki in so vsi deli posodobitve digitalno podpisani ter preverjeni s strani naprave pred procesom posodobitve), *avtentikacija* (predvsem opozarjajo na spremembo privzetih gesel ob prvi namestitvi, kjer šibka gesla niso dovoljena; ter poskrbeti za varovanje gesel in vzpostavitev avtorizacijskih shem, ki so drugačne za vsako napravo posebej), *avtorizacija*, *sistem dostopne kontrole*, *šifriranje za zagotovitev CIA* (zaupnost, celovitost, dostopnost), *varne in zaupanja vredne komunikacije*, *varno upravljanje vhodnih in izhodnih naprav*, *sistem za zapisovanje poročil o uporabi in dostopih*, *nadzorovanje* (predvsem za zaznavanje škodljive programske opreme in odkrivanje napak v celovitosti podatkov, ki jih naprava ima).

Symantec (2017) v svojem poročilu podaja podobne napotke, vendar dodaja, da je pred nakupom dobro vedeti, kaj naprava vse omogoča in kako je zaščitena, zato je dobro, da se pred nakupom pametnega avtomobila, kupca seznani z vsem, kar avtomobil uporablja, ter kako naj tovrstne funkcije upravlja za zagotavljanje čim večje zaščite. Poleg tega navaja, da naj uporabniki v svojih pametnih avtomobilih ne uporabljajo aplikacij, pridobljenih s strani tretjih oseb, ter naj ne odpirajo elektronskih sporočil s sumljivimi priponkami.

9 Metoda

Z namenom, da bi bolje spoznali poznavanje, razumevanje in dojemanje kibernetskih groženj pametnih avtomobilov pri voznikih, smo med slovenskimi vozniki izvedli spletno anketo na portalu »1ka.si« (Školc, 2018). Vprašalnik je bil aktiven od 22. 12. 2017 do 22. 3. 2018. Vozniki in voznice avtomobilov so bili o raziskavi informirani prek Facebook profilov ter spletnega foruma *Avtomobilizem.net*. Na anketo so odgovarjali polnoletni državljani Republike Slovenije. Značilnosti anketiranih so prikazane v tabeli 2. V vzorcu je bilo dve tretjini (66,4 %) žensk in več kot polovica (54,6 %) je bila starih med 21 in 30 let. V vzorec smo zajeli večinoma (87,9 %) voznike avtomobilov, ki so vsaj občasni vozniki. To so vozniki, ki so pri pogostosti vožnje odgovorili, da vozijo »včasih«, »pogosto« ali »zelo pogosto«. Zaradi velike razdrobljenosti odgovorov po regiji bivanja smo tvorili dve kategoriji odgovorov, »Osrednjeslovenska regija« in ostale regije[14]. Dobra tretjina (35,5 %) anketirancev prihaja iz Osrednjeslovenske regije, ostali iz ostalih regij. Med temi je bilo največ anketiranih iz Gorenjske regije (10,7 %), sledijo anketirani iz Podravske regije (10 %), Savinjske regije (6,4 %), Koroške regije (4,3 %),

[14] Ker je le-ta vsebovala največje število enot

Goriške regije (3,6 %), Obalno-kraške regije (2,9 %), Zasavske regije (2,1 %), Pomurske regije (2,1 %), Spodnjeposavske regije (1,4 %) ter Notranjsko-kraške regije (1,4 %). Anketirane smo po izobrazbi uvrstili v dve skupini, tiste z vsaj visoko šolo in ostale. Prvih je bilo v vzorcu 38,3 %, drugih 61,7 % (tabela 2).

Tabela 2: Značilnosti vzorca anketiranih voznikov avtomobilov

Demografske značilnosti		**f**	**%**
Starost (*n* = 108)	Manj kot 20	12	11,1
	21–30	59	54,6
	31–40	19	17,6
	Več kot 40	18	16,7
Spol (*n* = 107)	ženske	71	66,4
	Moški	36	33,6
Pogostost vožnje (*n* = 140)	Vozi redko oz. nikoli	17	12,1
	Vsaj občasni voznik	123	87,9
Izobrazba (*n* = 107)	Največ višja šola	66	61,7
	Visoka šola ali več	41	38,3
Regija (*n* = 107)	Ostale regije	69	64,5
	Osrednjeslovenska regija	38	35,5

V vprašalniku so vprašanja postavljena tako, da iz rezultatov dobimo vpogled v poznavanje in uporabo varnostnih rešitev ter zavedanje groženj, ki pretijo ob uporabi pametnih avtomobilov in njihovih povezljivosti z drugimi napravami. Vprašanja so bila merjena na 5-stopenjski Likertovi lestvici strinjanja z vrednostmi od 1 do 5, pri čemer 1 pomeni Nikakor se ne strinjam, 5 pa Popolnoma se strinjam. Vsebinski sklopi vprašanj so bili štirje, in sicer varnost povezljivosti, verjetnost zlorabe pametnega avtomobila, verjetnost kraje podatkov ter zadovoljstvo uporabnikov s pametnimi avtomobili. Analiza podatkov je vsebovala preverbo veljavnosti in zanesljivosti merjenja posameznih vsebinskih sklopov vprašalnika. Veljavnost merjenja smo ugotavljali z eksploratorno faktorsko analizo, zanesljivost s Cronbachovim koeficientom α. Povezanost med občutkom ogroženosti za krajo podatkov ter pogostostjo vožnje, nekaterimi demografskimi podatki in zadovoljstvom z uporabo avtomobila smo ugotavljali z večkratno linearno regresijo. Kot statistično značilne povezave smo upoštevali tiste z vrednostjo $p < 0,05$. Analiza podatkov je bila narejena s programskim orodjem SPSS, verzija 24.

10 Rezultati

V nadaljevanju so prikazani rezultati preverjanja veljavnosti merjenja štirih vsebinskih sklopov vprašalnika. Prvi sklop trditev v vprašalniku meri varnost povezljivosti. Anketirancem se zdi najbolj varna povezljivost z GPS sistemi (M = 3,45; SD = 0,95), sledijo povezljivosti: z mobilnimi napravami (M = 3,13; SD = 0,85), z drugimi pametnimi avtomobili (M = 2,96; SD = 0,89), s pametnimi domovi (M = 2,95; SD = 0,91), z brezžičnimi omrežji (M = 2,91; SD = 0,88) ter povezljivost s pametnimi mesti na zadnjem mestu (M = 2,87; SD = 0,85) Podatki so ustrezni za faktorsko analizo (KMO = 0,80; Bartlettov test sferičnosti: $\chi^2 = 458.72$; p =0,00). Z enim faktorjem pojasnimo 67,8 % variabilnosti merjenih spremenljivk. Vse trditve imajo na faktorju visoke uteži (razpon uteži je v intervalu 0,70–0,90). S trditvami torej ustrezno posredno merimo konstrukt varnost povezljivosti. Tvorimo sestavljeno spremenljivko, faktor, kot povprečno vrednosti trditev, ki faktor posredno merijo. Opis nove spremenljivke je podan v zadnji vrstici tabele. Vrednost Cronbachovega koeficienta α z vrednostjo 0,92 kaže na visoko zanesljivost merjenja. Vrednosti koeficienta višje od 0,60 pomenijo sprejemljivo zanesljivost, višje od 0,70 pa ustrezno zanesljivost merjenja (Hair, Anderson, Tatham in Black, 2006). Ustrezna zanesljivost merjenja je odraz močnih korelacij med spremenljivkami, ki merijo isti konstrukt (tabela 3).

Tabela 3: Faktorska analiza – Varnost povezljivosti

***F1*: Varnost povezljivosti**			
Cronbachov Alfa koeficient: 0,92			
Odstotek pojasnjene variance: 67,8			
Kaiser-Meyer-Olkinov koeficient ustreznosti vzorčenja: 0,80			
Barlettov test sferičnosti (χ^2): 458,72			
Vrednost $p < 0,001$			
Povezljivost pametnih avtomobilov z/s:	*F1*	*M**	*SD**
mobilnimi napravami je varna.	0,82	3,13	0,85
brezžičnimi omrežji je varna.	0,84	2,91	0,88
GPS sistemi je varna.	0,70	3,45	0,95
drugimi pametnimi avtomobili je varna.	0,83	2,96	0,89
pametnimi domovi je varna.	0,85	2,95	0,91
pametnimi mesti je varna.	0,90	2,87	0,85
Povprečna vrednost faktorja: M = 3,05			
Standardni odklon faktorja: SD = 0,76			

* M = aritmetična sredina; SD = standardni odklon

Drugi sklop trditev v vprašalniku meri verjetnost zlorabe pametnega avtomobila. Anketirancem se zdi najverjetneje to, da jim preko pametnega avtomobila lahko sledijo (M = 3,87; SD = 0,96), sledi oddajanje digitalnih podatkov brez uporabnikove vednosti (M = 3,63; SD = 1,04), prestrezanje komuni-

kacije v avtomobilu (*M* = 3,57; *SD* = 0,99), okužbe z zlonamerno kodo (*M* = 3,50; *SD* = 1,06), nadzor nad avtomobilom s strani tretje osebe (*M* = 3,47; *SD* = 1,05), kraja digitalnih podatkov iz avtomobila (*M* = 3,41; *SD* = 0,97) ter odtujitev pametnega avtomobila (*M* = 3,40; *SD* = 0,98) na zadnjem mestu. Podatki so ustrezni za faktorsko analizo (*KMO* = 0,91; Bartlettov test sferičnosti: χ^2 = 522,85; $p < 0{,}001$). Z enim faktorjem pojasnimo 63,9 % variabilnosti merjenih spremenljivk. Vse trditve imajo na faktorju visoke uteži (razpon uteži je v intervalu 0,67–0,86). S trditvami torej ustrezno posredno merimo konstrukt verjetnost zlorabe pametnega avtomobila. Opis nove spremenljivke je podan v zadnji vrstici tabele. Vrednost Cronbachovega koeficienta α z vrednostjo 0,92 kaže na visoko zanesljivost merjenja (tabela 4).

faktorsko analizo (*KMO* = 0,84; Bartlettov test sferičnosti: χ^2 = 735,03; p = 0,00). Z enim faktorjem pojasnimo 70 % variabilnosti merjenih spremenljivk. Vse trditve imajo na faktorju visoke uteži (razpon uteži je v intervalu 0,74–0,92). S trditvami torej ustrezno posredno merimo konstrukt verjetnost zlorabe pametnega avtomobila. Opis nove spremenljivke je podan v zadnji vrstici tabele. Vrednost Cronbachovega koeficienta α z vrednostjo 0,93 kaže na visoko zanesljivost merjenja (tabela 5).

Tabela 4: Faktorska analiza – Verjetnost zlorabe pametnega avtomobila

***F2:* Verjetnost zlorabe pametnega avtomobila**			
Cronbachov Alfa koeficient: 0,92			
Odstotek pojasnjene variance: 63,85			
Kaiser-Meyer-Olkinov koeficient ustreznosti vzorčenja: 0,91			
Barlettov test sferičnosti (χ^2): 522,85			
Vrednost $p < 0{,}001$			
	F1	*M**	*SD**
Verjetnost za odtujitev pametnega avtomobila je velika.	0,68	3,40	0,98
Verjetnost, da mi lahko ukradejo digitalne podatke iz pametnega avtomobila, je velika.	0,77	3,41	0,97
Verjetnost, da mi preko pametnega avtomobila lahko sledijo, je velika.	0,81	3,87	0,96
Verjetnost za prevzem nadzora nad pametnim avtomobilom s strani tretje osebe je velika.	0,78	3,47	1,05
Verjetnost za oddajanje digitalnih podatkov iz pametnega avtomobila brez moje vednosti je velika.	0,84	3,63	1,04
Pri uporabi pametnega avtomobila je velika verjetnost, da mi prestrezajo komunikacije (podatkov, klicev ...).	0,85	3,57	0,99
Verjetnost, da se pametni avtomobil lahko okuži z zlonamerno kodo (Ransomware, malware, spyware, virusi, trojanski konji ...), je velika.	0,86	3,50	1,06
Povprečna vrednost faktorja: *M* = 3,55 Standardni odklon faktorja: *SD* = 0,84			

* *M* = aritmetična sredina; *SD* = standardni odklon

Tretji sklop trditev v vprašalniku meri stopnjo ranljivosti podatkov z uporabo pametnega avtomobila. Anketirancem se zdi najvišja stopnja ranljivosti stikov (*M* = 3,33; *SD* = 1,12), sledijo ranljivosti gesel za dostop do različnih sistemov (*M* = 3,23; *SD* = 1,27), fotografij in/ali video vsebin (*M* = 3,22; *SD* = 1,04), dokumentov (*M* = 3,18; *SD* = 1,11), certifikatov (*M* = 3,17; *SD* = 1,24) ter najmanjša stopnja ranljivosti koledarskih vnosov (*M* = 2,97; *SD* = 1,07). Podatki so ustrezni za

Tabela 5: Faktorska analiza – Ranljivost podatkov z uporabo pametnega avtomobila

***F3*: Ranljivost podatkov z uporabo pametnega avtomobila**			
Cronbachov Alfa koeficient: 0,93			
Odstotek pojasnjene variance: 70,00			
Kaiser-Meyer-Olkinov koeficient ustreznosti vzorčenja: 0,84			
Barlettov test sferičnosti (χ^2): 735,03			
Vrednost $p < 0{,}001$			
	F1	*M**	*SD**
Fotografije in/ali video vsebine	0,74	3,22	1,04
Dokumente (službene, zasebne, tajne ...)	0,92	3,18	1,11
Koledarske vnose (službeni, zasebni)	0,81	2,97	1,07
Certifikate (banka, dostop do poslovnih sistemov idr.)	0,87	3,17	1,24
Gesla ter PIN številke za dostop do različnih sistemov (mobilno bančništvo, poslovni sistemi, kartice ...)	0,87	3,23	1,28
Stike (tel. številke, e-maili ...)	0,79	3,33	1,12
Povprečna vrednost faktorja: $M = 3{,}20$ Standardni odklon faktorja: $SD = 1{,}00$			

* *M* = aritmetična sredina; *SD* = standardni odklon

Četrti sklop trditev v vprašalniku meri zadovoljstvo anketiranih z uporabo pametnega avtomobila. Anketirani so najbolj zadovoljni z udobjem vožnje ($M = 3{,}76$; $SD = 0{,}99$), sledijo možnost zlorabe podatkov preko povezanih naprav ($M = 3{,}64$; $SD = 1{,}11$), lažje upravljanje avtomobila ($M = 3{,}51$; $SD = 1{,}00$), zabavnejša vožnja ($M = 3{,}11$; $SD = 1{,}25$) ter najmanj zadovoljni z dodatnim bremenom oz. skrbjo ($M = 3{,}04$; $SD = 1{,}07$). Trditev, da je možnost zlorabe podatkov preko povezanih naprav, nima visoke uteži na faktorju, zato jo iz nadaljnje analize izpustimo. Podatki so ustrezni za faktorsko analizo ($KMO = 0{,}71$; Bartlettov test sferičnosti: $\chi^2 = 142{,}97$; $p = 0{,}00$). Z enim faktorjem pojasnimo 37,5 % variabilnosti merjenih spremenljivk. Vse trditve imajo na faktorju visoke uteži (razpon uteži je v intervalu 0,55–0,76). S trditvami torej ustrezno posredno merimo konstrukt ranljivost podatkov z uporabo pametnega avtomobila. Opis nove spremenljivke je podan v zadnji vrstici tabele. Vrednost Cronbachovega koeficienta α z vrednostjo 0,76 kaže na ustrezno zanesljivost merjenja (tabela 6).

Tabela 6: Faktorska analiza – Zadovoljstvo z uporabo pametnega avtomobila

***F4*: Zadovoljstvo z uporabo pametnega avtomobila**			
Cronbachov Alfa koeficient: 0,76			
Odstotek pojasnjene variance: 37,53			
Kaiser-Meyer-Olkinov koeficient ustreznosti vzorčenja: 0,71			
Barlettov test sferičnosti (χ^2): 142,97			
Vrednost $p < 0{,}001$			
	*F1**	*M***	*SD***
Lažje upravljanje z avtomobilom	0,67	3,51	0,99
Zabavnejšo vožnjo	0,71	3,11	1,26
Udobnejšo vožnjo	0,77	3,76	0,99
Dodatno breme, skrb (R)	0,55	3,04	1,07
Možnost zlorabe podatkov preko povezanih naprav (R)		3,64	1,11
Povprečna vrednost faktorja: $M = 3{,}34$ Standardni odklon faktorja: $SD = 0{,}82$			

(R) – obrnjena spremenljivka (Recode)
* prikazane so uteži > 0,40
** *M* = aritmetična sredina; *SD* = standardni odklon

Tabela 7 prikazuje rezultat treh večkratnih linearnih regresijskih modelov s tremi različnimi odvisnimi spremenljivkami: ranljivost podatkov z uporabo pametnega avtomobila, verjetnost zlorabe pametnega avtomobila, varnost povezljivosti in naslednjimi neodvisnimi spremenljivkami: pogostost vožnje, regija, spol, starost, izobrazba in zadovoljstvo z uporabo avtomobila. Rezultati kažejo, da je ob kontroli na ostale spremenljivke v modelu z ranljivostjo podatkov zaradi uporabe pametnega avtomobila povezana frekvenca vožnje (Std. B = –0,21; $p = 0{,}044$). Negativna vrednost standardiziranega regresijskega koeficienta pomeni, da se občutek ranljivosti podatkov zaradi uporabe pametnega avtomobila s frekvenco vožnje zmanjšuje. Vsaj občasni vozniki se tako manj zavedajo ranljivosti podatkov zaradi uporabe pametnega avtomobila kot vozniki, ki avto uporabljajo le redko oz. nikoli.

Ob kontroli na ostale spremenljivke v modelu sta tako ocena verjetnosti zlorabe pametnega avtomobila kot varnost povezljivosti povezani z zadovoljstvom z uporabo avtomobila. Bolj zadovoljnim uporabnikom avtomobila se zdi verjetnost zlorabe pametnega avtomobila statistično značilno nižja kot manj zadovoljnim uporabnikom (Std b = –0,25; $p = 0{,}010$). Nakazana je tudi negativna povezava med frekvenco vožnje in verjetnostjo zlorabe pametnega avtomobila (Std b = –0,187; $p = 0{,}084$). Vsaj občasni vozniki ocenjujejo verjetnost zlorabe pametnega avtomobila kot nižjo v primerjavi z vozniki, ki vozijo redko ali sploh ne. Zadovoljni vozniki ocenjujejo povezljivost avtomobila kot varnejšo v primerjavi z manj zadovoljnimi vozniki (Std. b = 0,28; $p = 0{,}004$) kar je skladno s predhodnimi ugotovitvami.

Tabela 7: Dejavniki, povezani z zaznavanjem ogroženosti podatkov zaradi uporabe pametnega avtomobila (večkratna linearna regresija)

	***F3*: Ranljivost podatkov zaradi uporabe pam. avtomobila**	***F2*: Verjetnost zlorabe pam. Avtomobila**	***F1*: Varnost povezljivosti**
	Std. b (vrednost *p*)*	Std. b (vrednost *p*)*	Std. b (vrednost *p*)*
Vsaj občasni voznik	–0,21 (0,044)	–0,20 (0,084)	0,03 (0,797)
Osrednja regija	0,1 (0,337)	–0,05 (0,580)	–0,04 (0,688)
Visoka izobrazba	–0,02 (0,877)	0,03 (0,752)	0,07 (0,449)
Starost	0,04 (0,719)	0,00 (0,998)	–0,01 (0,906)
Zadovoljstvo z uporabo avtomobila	–0,04 (0,692)	–0,25 (0,010)	0,28 (0,004)

* Std. b = standardizirani regresijski koeficient

11 Diskusija

Z izbranimi metodami in pojasnjenimi rezultati smo dosegli namen in cilje, ki smo jih želeli v prispevku prikazati. S teoretičnimi izhodišči smo prikazali, da se avtomobili povezujejo s kibernetskim prostorom (ENISA, 2016) in so posledično ranljivi na grožnje, ki pretijo v kibernetskem prostoru (ENISA, 2016; Nakrani, 2015). Kot taki so predmet kibernetske kriminalitete in posledično kazenske odgovornosti. Kazensko pravo omogoča kazenski pregon bistvenih uresničitev groženj, kakršne predvideva ENISA, saj je mogoče za to uporabiti obstoječe opredelitve kaznivih dejanj. Temeljni vprašanji, ki se pri tem pojavljata, sta razmejitev oziroma omejitev kazenske odgovornosti voznika pametnega avtomobila in tretjih oseb, ki vdrejo v informacijski sistem tega avtomobila, in razrešitev stekov med kaznivim dejanjem iz 221, člena KZ-1 (2012, 2015, 2016) ter drugimi upoštevnimi kaznivimi dejanji. Uporabnikovo dojemanje kibernetskih groženj in pametnega avtomobila kot dela kibernetskega prostora in interneta stvari je ključnega pomena pri zagotavljanju kibernetske varnosti in zmanjševanju kibernetske kriminalitete. Številni primeri že izvedenih kaznivih dejan, vezanih na krajo avtomobilov (Kolenc et al., 2013) in napadov na informacijske sisteme (Markelj in Završnik, 2016), dokazujejo, da se bo trend tveganj uresničitve kibernetske kriminalitete pri pametnih avtomobilih nadaljeval.

Na cestah bo vedno več pametnih avtomobilov (Meola, 2016), zato se bo stopnja varnosti njihove uporabe morala povišati, hkrati pa bo treba povišati prijaznost uporabe. Potrebna bo tako večja fizična varnost kot tudi informacijska varnost, saj je v več primerih z zlorabo informacijskega sistema že prišlo do oddaljenega upravljanja avtomobila, kar lahko pripelje do fizičnih poškodb voznika. Na podlagi rezultatov raziskave smo ugotovili, da se uporabnikom pametnih avtomobilov zdi najverjetneje, da jim preko pametnega avtomobila lahko sledijo, zato priporočamo, da se uporabnike pametnih avtomobilov ozavešča o načinih delovanja pametnega avtomobila pred nakupom le-tega. Rezultati nam prav tako pokažejo, da se s frekvenco uporabe pametnega avtomobila (vožnjo) občutek ranljivosti podatkov, do katerih ima pametni avtomobil dostop, zmanjšuje. Kar pomeni, da se vsaj občasni vozniki manj zavedajo ranljivosti podatkov zaradi uporabe pametnega avtomobila kot vozniki, ki avtomobil uporabljajo le redko oz. nikoli. Že Bernik in Meško (2011) ugotavljata, da se uporabniki kibernetskega prostora (kar vozniki pametnih avtomobilov so) manj zavedajo specifičnih oblik groženj, ki pretijo znotraj kibernetskega prostora. Ravno tako Markelj in Završnik (2016) ugotavljata uporabnikovo brezbrižnost do uresničitve kibernetskih groženj, kljub poznavanju varnostnih rešitev in njihovi neuporabi. Ugotovili smo tudi, da vsaj občasni vozniki v vzorcu ocenjujejo verjetnost zlorabe pametnega avtomobila kot nižjo v primerjavi z vozniki, ki vozijo redko oz. sploh ne, a je povezanost med frekvenco vožnje in oceno verjetnosti zlorabe pametnega avtomobila le mejno statistično značilna. Na podlagi omenjenih dejstev lahko ugotovimo, da se kljub vedno večji rabi kibernetskega prostora uporabniki pametnih avtomobilov slabo zavedajo pomena kibernetske varnosti in podatkov, s katerimi delujejo (predvsem tisti, ki pogosteje vozijo in so bolj zadovoljni z uporabo pametnega avtomobila). Rezultati raziskave nam pokažejo tudi, da vozniki, ki so s pametnim avtomobilom bolj zadovoljni, ocenjujejo povezljivost pametnega avtomobila s pametno napravo varnejšo v primerjavi s tistimi, ki so s pametnim avtomobilom manj

zadovoljni. Kar pomeni, da se prvim zdi uresničitev kibernetskega kriminala manj verjetna kot drugim. Zadovoljstvo s pametnim avtomobilom lahko povežemo tudi s številom kibernetsko varnostnih incidentov, povezanih s pametnimi avtomobili, posledicami (kibernetska kriminaliteta, kazenska odgovornost) in uporabnikovim poznavanjem le teh. Glede na trenutno majhno število medijsko izpostavljenih kibernetsko varnostnih incidentov, vezanih na pametne avtomobile, in malo strokovne literature, ki pojasni povezavo pametnega avtomobila z ostalim kibernetskim prostorom in poenoti dojemanje mobilne naprave, interneta, pametnih naprav in pametnega avtomobila, nas predhodno predstavljeni rezultati ne presenečajo.

Ocena verjetnosti zlorabe pametnega avtomobila in varnost povezljivosti sta povezani z zadovoljstvom z uporabo avtomobila, in sicer bolj zadovoljnim uporabnikom se zdi verjetnost zlorabe pametnega avtomobila nižja kot tistim, ki so z uporabo manj zadovoljni.

12 Zaključek

Pametni avtomobili so ena novejših tematik v svetu IoT in pametnih naprav, katerih področje je v Sloveniji neraziskano. Zadnje čase jim posvečamo vse več pozornosti, saj se grožnje in tveganja pametnim avtomobilom sorazmerno večajo z novostmi in uporabo le teh. Največja težava v varovanju pametnih avtomobilov pa je Infotainment domena oz. sistem, preko katerega se prikazuje in povezuje različne zabavne vsebine in naprave, ki jih kot vozniki sicer ne potrebujemo, vendar si jih želimo. Namreč preko tega nam lahko z zlonamerno kodo in/ali z našo nepazljivostjo, napadalci storijo večjo škodo, kot bi jo sicer storili, če bi nam vdrli v namizni računalnik (namesto zgolj ukradenih podatkov, ki so že tako velika škoda, saj je s tem lahko v nevarnosti naša identiteta, nam lahko z zlorabo avtomobila ogrožajo fizično zdravje in zdravje sopotnikov v avtomobilu). Slovensko kazensko pravo sicer večino uresničitev predvidenih groženj pametnim avtomobilom inkriminira kot kaznivo dejanje ali prekršek, kar, seveda ob upoštevanju temeljnih institutov kazenskega in prekrškovnega materialnega prava, omogoča njihov kazenski pregon. Ker pa bodo pametni avtomobili vedno bolj dostopni vsakomur, je pri varovanju voznikov in njihovih podatkov na mobilnih napravah, pomembno poleg zaščitnih mehanizmov v napravah in avtomobilih, zagotoviti ustrezno izobraževanje celotne populacije, ki se s pametnimi avtomobili srečuje v vsakodnevnem življenju. Namreč ne glede na vse je človek še vedno najšibkejši člen pri zagotavljanju informacijske varnosti splošno in v pametnih avtomobilih. V drugi vrsti pa je pomembno, da se naprave, ki jih uporabljajo tako vozniki kot pametni avtomobili sami (in so po navadi narejene pri več proizvajalcih), certificira in s tem zagotovi višjo stopnjo varnosti, ter to pri nakupu oziroma prodaji pametnega avtomobila tudi ustrezno zagotoviti in s tem seznaniti kupca. Pametne avtomobile je treba uporabljati premišljeno in varno kot vse druge mobilne naprave in računalnike, ki so povezani v skupen kibernetski prostor.

Literatura

1. Anderson, M. J., Kalra, N., Stanley, D. K., Sorensen, P., Samaras, C. in Oluwatola, A. O. (2014). Brief history and current state of autonomous vehicles. V J. M. Anderson, N. Kalra, K. D. Stanley, P. Sorensen, C. Samaras in O. A. Oluwatola (ur.), *Autonomous vehicle technology: A Guide for policymakers* (str. 55–74). Santa Monica: RAND Corporation.
2. Barret, J. (2012). *The Internet of Things TEDxCIT*. Pridobljeno na https://www.youtube.com/watch?v=QaTIt1C5R-M
3. Bavcon, L. Šelih, A., Ambrož, M., Filipčič, K. in Korošec, D. (2013). *Kazensko pravo, splošni del.* Ljubljana: Uradni list RS.
4. Beltov, M. (10. 7. 2016). Smart cars and security – The game of risks. *Bestsecuritysearch.com*. Pridobljeno na https://bestsecuritysearch.com/smart-cars-security-game-risks/
5. Bernik, I. in Markelj, B. (2014). Zagotavljanje varnosti informacij z razumevanjem uporabnikovega ravnanja z mobilno napravo. *Varstvoslovje, 16*(1), 5–15.
6. Bernik, I. in Meško, G. (2011). Internetna študija poznavanja kibernetskih groženj in strahu pred kibernetsko kriminaliteto. *Revija za kriminalistiko in kriminologijo, 62*(3), 242–252.
7. Browne, W. (2016). *Internet of things devices increases cyber vulnerability of vehicles* (Magistrska naloga). Utica: Utica College.
8. Chui, M., Löffler, M. in Roberts, R. (9. 3. 2010) The Internet of things. *Mckinsey.com*. Pridobljeno na https://www.mckinsey.com/industries/high-tech/our-insights/the-internet-of-things
9. Constantin, L. (16. 11. 2017). Researchers hack car infotainment system and find sensitive user data inside. *Motherboard.vice.com*. Pridobljeno na https://motherboard.vice.com/en_us/article/3kvw8y/researchers-hack-car-infotainment-system-and-find-sensitive-user-data-inside
10. Eman, K. in Franca, B. (2016). Trgovanje z električno in elektronsko opremo – problem moderne družbe. *Revija za kriminalistiko in kriminologijo, 67*(3), 248–261.
11. Eskandarian, A. (2012a). *Handbook of intelligent vehicles*. London: Springer-Verlag.
12. Eskandarian, A. (2012b). Introduction to intelligent vehicles. V A. Eskandarian (ur.), *Handbook of intelligent vehicles* (str. 7–9). London: Springer-Verlag.
13. European Union Agency For Network And Information Security [ENISA]. (2016). *Cyber security and resilience of smart cars: Good practises and recommendations.* Pridobljeno na https://www.enisa.europa.eu/publications/cyber-security-and-resilience-of-smart-cars/at_download/fullReport
14. European Union Agency For Network And Information Security [ENISA]. (2017). *Baseline security recommendations for IoT in the context of Critical Information Infrastructures.* Pridobljeno na https://www.enisa.europa.eu/publications/baseline-security-recommendations-for-iot/at_download/fullReport
15. Georgiadis, K. C., Polatidis, N., Mouratidis, H. in Pimenidis, E. (2017). A method for privacy-preserving collaborative filtering reccommendations. *Journal of Universal Computer Science, 23*(2), 146–166.

16. Greenberg, A. (8. 1. 2016). The Jeep hackers are back to prove car hacking can get much worse. *Wired.com*. Pridobljeno na https://www.wired.com/2016/08/jeep-hackers-return-high-speed-steering-acceleration-hacks/
17. Hair, J., Anderson, R., Tatham, R. in Black, W. (2006) *Multivariate data analysis.* Upper Saddle River: Pearson/Prentice Hall, Inc.
18. Hartfield, S. R. (2017). *21st century automobiles: Vulnerabilities, threats, cyber security and digital forensics* (Magistrska naloga). Utica: Utica College.
19. Heberle, A., Löwe, W., Gustafsson, A. in Vorrei, Ö. (2017). Digitalization canvas – towards identifying digitalization use cases and projects. *Journal of Universal Computer Science, 23*(11), 1070–1097.
20. Japelj, B. (2015). Kriminaliteta v Sloveniji leta 2014. *Revija za kriminalistiko in kriminologijo, 66*(2), 130–152.
21. Japelj, B. (2016). Kriminaliteta v Sloveniji leta 2015. *Revija za kriminalistiko in kriminologijo, 67*(2), 140–170.
22. Kazenski zakonik [KZ-1]. (2012, 2015, 2016, 2017). *Uradni list RS*, (50/12, 54/15, 6/16, 27/17).
23. Kolenc, T., Kebe, J. in Bukovnik, A. (2013). Kriminaliteta v Sloveniji v letu 2012. *Revija za kriminalistiko in kriminologijo, 64*(2), 95–121.
24. Kolenc, T., Kebe, J. in Bukovnik, A. (2014). Kriminaliteta v Sloveniji v letu 2013. *Revija za kriminalistiko in kriminologijo, 65*(3), 175–206.
25. Lamberger, I., Slak, B. in Dobovšek, B. (2013). Kriminalistično preiskovanje spletnih goljufij s predplačili. *Revija za kriminalistiko in kriminologijo, 64*(2), 195–203.
26. Markelj, B. in Završnik, A. (2016). Kibernetska korporativna varnost mobilnih naprav: zavedanje uporabnikov v Sloveniji. *Revija za kriminalistiko in kriminologijo, 67*(1), 44–60.
27. McAfee. (2017). *Automotive security best practises.* Pridobljeno na: https://www.mcafee.com/us/resources/white-papers/wp-automotive-security.pdf
28. Meola, A. (10. 12. 2016). Automotive industry trends: iot connected smart cars & vehicles. *Businessinsider.com.* Pridobljeno na http://www.businessinsider.com/internet-of-things-connected-smart-cars-2016-10
29. Mijalković, S., Bošković, G., Vuković, S. in Vučković, G. (2016). Trendi tatvin motornih vozil v Republiki Srbiji in drugih evropskih državah. *Revija za kriminalistiko in kriminologijo, 67*(1), 26–43.
30. Nakrani, P. K. (2015). *Smart car technologies: A comprehensive study of the state of the art with analysis and trends* (Magistrska naloga). Tucson: University of Arizona.
31. Pacheco, J., Satam, S., Hariri, S., Grijalva, C. in Berkenbrock, H. (15. 11. 2016). *IoT security development framework for building trustworthy smart car services.* Pridobljeno na https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=7745481
32. Payne III., L. R. (2017). *Vehicle manipulation and forensics* (Magistrska naloga). Utica: Utica College.
33. Pearson, T. E. (2017). *The need for encryption and secure systems within vehicles* (Magistrska naloga). Utica: Utica College.
34. Peppet, S. R. (2014). *Regulating the Internet of things: First steps toward managing discrimination, privacy, security, and consent. Texas Law Review, 93*, 85–178.
35. Rouse, M. in Wright, R. (2017). *Definition: Botnet.* Pridobljeno na https://searchsecurity.techtarget.com/definition/botnet
36. Schober, S. (15. 4. 2016). Cybersecurity and the future of smart cars. *ibmbigdatahub.com.* Pridobljeno na http://www.ibmbigdatahub.com/blog/cybersecurity-and-future-smart-cars
37. Schorer, M. (2015). *Connected car business brief series|02.* Pridobljeno na https://www.vmware.com/ciovantage/wp-content/uploads/2015/12/ConnectedCar-2-Security.pdf
38. Schwartz, P., M. (2004). Property, privacy, and personal data. *Harward Law Review, 117*, 2056–2128.
39. *Security and Privacy in Your Car Act* [SPY Car Act]. (2015). Pridobljeno na https://www.congress.gov/bill/114th-congress/senate-bill/1806
40. Silberg, G., Plesco, R., Rotman, D. in Le, D. (2016). *Your connected car is talking. Who's listening?* Pridobljeno na: https://assets.kpmg.com/content/dam/kpmg/id/pdf/2017/04/id-your-connected-car-is-talking.pdf
41. Smith, L. J. (17. 10. 2017). Car thieves steal £50,000 BMW in seconds – Is your car at risk too? *Express.co.uk.* Pridobljeno na https://www.express.co.uk/life-style/cars/866987/car-theft-hack-keyless-entry-video-BMW-stolen
42. Symantec. (2017). *Internet security threat report.* Pridobljeno na https://www.symantec.com/content/dam/symantec/docs/reports/istr-22-2017-en.pdf
43. Školc, G. (2018). *Informacijska varnost pri rabi pametnih avtomobilov* (Magistrska naloga). Ljubljana: Fakulteta za varnostne vede.
44. Ward, B, D. (2017). *Automotive cybersecurity -Redifining war driving* (Magistrska naloga). Utica: Utica College.
45. Zakon o varstvu osebnih podatkov [ZVOP-1]. (2004, 2005, 2007). *Uradni list RS,* (86/04, 113/05, 51/07, 67/07, 94/07).
46. Završnik, A. (2010). Tehnično nadzorovanje vsakodnevnega življenja – postdisciplinske teoretične perspektive. *Revija za kriminalistiko in kriminologijo, 61*(2), 178–190.
47. Završnik, A. in Sedej, A. (2012). Spletno in mobilno nadlegovanje v Sloveniji. *Revija za kriminalistiko in kriminologijo, 63*(4), 263–280.
48. Zurkus, K. (25. 3. 2015). Are smart cars putting our safety at risk? *Csoonline.com.* Pridobljeno na https://www.csoonline.com/article/2900654/data-protection/are-smart-cars-putting-our-safety-at-risk.html

Smart Cars and Cybercrime

Blaž Markelj, Ph.D., Assistant Professor, Faculty of Criminal Justice and Security, University of Maribor, Slovenia.
E-mail: blaz.markelj@fvv.uni-mb.si

Gašper Školc, M.A., Faculty of Criminal Justice and Security, University of Maribor, Slovenia. E-mail: gasper.skolc@student.um.si

Vanja Ida Erčulj, M.A., Lecturer, Faculty of Criminal Justice and Security, University of Maribor, Slovenia.
E-mail: vanja.erculj@fvv.uni-mb.si

Sabina Zgaga, Ph.D., Advisor to the Constitutional Court of the Republic of Slovenia and Assistant Professor, Faculty of Law, University of Ljubljana, Slovenia. E-mail: sabina.zgaga@us-rs.si

In the past, cars were considered only as means of transport, which centers were the driver, cars, and their interaction with traffic. For achieving safety, the driver's capability to drive in various conditions and the technical perfection of the cars were of utmost importance. However, with developing technology, the car has become a part of the Internet of things. It has become the means, which connects to cyber-space, functions on the basis of data, acquired from the environment and it connects to other smart devices, such as the wide variety of mobile devices. With such development, the car has become vulnerable to cyber-criminality as well, and while connecting to cyber-space, the car has become vulnerable to cyber-threats. The aim of the paper is to present the security of smart car user's data, to emphasize the awareness of this topic with smart car users (both private and business) as well as to point to certain criminal law issues relative to this topic. The first part of the paper includes information security issues regarding smart cars, which relate to criminal law elements, and threats, which could result in cyber-crime, are described. The second part of the paper discusses previous research in this area, which shows how well the participants are aware of information security of smart cars.

Keywords: smart cars, mobile devices, information security, cybercrime, criminal responsibility

UDC: 004.056:629.331