Revija za kriminalistiko in kriminologijo / Ljubljana 69 / 2018 / 1, 15–29

Kibernetska varnost in kibernetska kriminaliteta uporabnikov mobilnih naprav v Sloveniji[1]

Blaž Markelj[2], Sabina Zgaga[3]

Informacijska tehnologija (vključno z mobilnimi napravami) je omogočila širjenje novih oblik kriminalitete (kibernetska kriminaliteta). Povečana uporaba mobilnih naprav, tako za zasebne in poslovne kakor tudi za kriminalne namene, in vedno večja uporabnost mobilnih naprav se kažeta v razvoju kazenskega prava, ki mora urejati tudi ustrezne opredelitve kaznivih dejanj in pravila splošnega dela, ki mobilno napravo obravnavajo kot predmet napada in/ali sredstvo za izvedbo kaznivega dejanja. V prvem delu prispevka so najprej predstavljene glavne ugotovitve raziskave, ki je bila opravljena v poslovnem sektorju med 34 slovenskimi organizacijami, in sicer o rabi mobilnih naprav, ogroženosti ter uporabi ustreznih oblik zaščite. Ti podatki prikazujejo dejansko stanje ogroženosti mobilnih naprav v Sloveniji ter možnosti za nastanek varnostnega incidenta in s tem izvedbo upoštevnih kaznivih dejanj. Drugi del prispevka obravnava problematiko z vidika kazenskega prava; najprej na podlagi ureditve ustreznih kaznivih dejanj v *Kazenskem zakoniku* (KZ-1, 2012), pozneje pa še na podlagi prikaza uradnih statističnih podatkov Policije ter Statističnega urada Republike Slovenije o procesiranju teh kaznivih dejanj. V sklepu je ponujena rešitev za izboljšanje kibernetske varnosti mobilnih naprav in s tem zmanjšanje možnosti uresničitve kibernetske kriminalitete – model vpeljave mobilnih naprav v organizacijsko okolje, upoštevajoč elemente informacijske varnosti ter raznolikosti in potreb delovnih procesov.

Ključne besede: mobilne naprave, kibernetska varnost, kibernetska kriminaliteta, kazensko pravo

UDK: 343.3/.7:004

1 Uvod

Spreminjajoče se svetovno družbeno okolje nam vedno bolj dokazuje, da je varnost dobrina, ki postaja redkost. Za zagotavljanje varnosti je treba poznati tudi grožnje oziroma vire njenega ogrožanja. Poznavanje teh je ključno pri oblikovanju nacionalne varnostne politike (Sotlar, 2008), odsotnost groženj pa lahko opredelimo tudi kot stanje varnosti (Grizold, 1992; Sotlar in Tominc, 2012). Pomembnost varnosti za normalno življenje in delovanje dokazujejo številne znanstvene, strokovne in medijske objave o varnosti. Z vprašanjem varnosti na splošno se z različnih vidikov ukvarjajo znanstveniki različnih disciplin; denimo Dimc in Dobovšek (2010), Meško in Bernik (2011), Sotlar (2008), Sotlar in Tominc (2012), Markelj in Bernik (2011), Wall (2008a), Van Duyne (2009), Vander Beken in Van Daele (2009) ter Schjolberg, (2010). Varnost je pogosto obravnavana z vidika posameznika, saj je ta v središču problema, njegovega delovanja in odzivov na vplive okolja, kar nakazujejo raziskave (npr. Meško in Bernik (2011), raziskava o strahu pred kibernetsko kriminaliteto; Markelj in Bernik (2011), raziskava o uporabi mobilnih naprav med mladimi; ter Markelj in Završnik (2016), raziskava o zavedanju uporabnikov mobilnih naprav v slovenskih organizacijah). Prav na podlagi okoljskih vplivov lahko problematiko varnosti razdelimo na posamezna strokovna področja. Eno od pomembnejših je informacijska varnost, delovanje uporabnika v kibernetskem prostoru.

Vedno večja priljubljenost kibernetskega prostora, vse pogostejša raba informacijskih tehnologij in posledično tudi vedno večji vpliv teh na človeka (vpliv je lahko pozitiven, če povečuje delovno uspešnost, ali negativen, če omogoča kibernetsko kriminaliteto) nakazujejo potrebo po poglobljenem raziskovanju medsebojnega učinkovanja človeka oziroma uporabnika in tehnologije. Europolovo (2013) poročilo *Serious and Organised Crime Threat Assessment* za leto 2013 opredeljuje razvoj mobilnih naprav, možnost nenehne komunikacije ter razvoj škodljive programske opreme predvsem kot sredstvo, ki organizirani kriminaliteti omogoča še hitrejši razvoj ter širjenje njenih mrež in možnosti zlorab. Poročilo omenja tudi hiter razvoj škodljive programske opreme za mobilne naprave, ki za kibernetsko kriminaliteto pomeni možnost za širjenje delovanja, kar je velika nevarnost za uporabnike mobilnih naprav ter tudi za celotno družbo.

---

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

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

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

Rezultati raziskav, v katerih se proučujejo uporaba sodobnih tehnologij (Dimc in Dobovšek, 2010), kibernetska kriminaliteta in strah pred njo (Meško in Bernik, 2011), omogočajo opredelitev smernic za varnejše delovanje človeka v resničnem in tudi kibernetskem svetu. Informacijska tehnologija je v preteklih 50 letih temeljito spremenila delovne okoliščine, komunikacijske poti in načine vzpostavljanja stikov; omogočila je napredek v številnih gospodarskih panogah in spodbudila razvoj novih.

Z razvojem informacijskih tehnologij so se meje kriminalitete še bolj zabrisale, saj se je poslovno in osebno okolje rabe podatkov in tehnologije popolnoma združilo in tako so kriminalna dejanja postala še težje določljiva in sledljiva. Za kriminaliteto se je oblikoval svet novih priložnosti. *Konvencija Sveta Evrope o kibernetski kriminaliteti* (Svet Evrope, 2004) določa osnovne okvire za njeno razumevanje in preganjanje, problematično pa je, da je ta dejanja še vedno težko opredeliti, saj je to odvisno tudi od dojemanja posameznikov (Wall, 2008b). Zaradi eksponentnega razvoja tehnologije in povečevanja števila uporabnikov storitev, ki jih ponuja kibernetski prostor, se čedalje jasneje kaže tudi, kako pomembna je postala informacijska varnost. Strokovnjaki, ki se ukvarjajo z njenim raziskovanjem, zdaj namenjajo največ pozornosti prav mobilnim napravam in načinom njihove rabe za zasebne in poslovne namene.

Povečana uporaba mobilnih naprav, tako za zasebne in poslovne kakor tudi za kriminalne namene, pa tudi vedno večja uporabnost teh naprav vplivata tudi na kazensko pravo, in sicer pri odkrivanju, preiskovanju in dokazovanju kaznivih dejanj v kazenskem postopku, v katerem potrebujemo ustrezna pooblastila za preiskovanje teh kaznivih dejanj, in v kazenskem materialnem pravu, ki mora vsebovati ustrezne opredelitve kaznivih dejanj in pravila splošnega dela, ki mobilno napravo obravnavajo kot predmet napada in/ali sredstvo za izvedbo kaznivega dejanja.

Namen članka je predstaviti varnostno problematiko in tveganja, ki nastajajo ob rabi mobilnih naprav v organizacijah, v povezavi s pravnimi zakoni Republike Slovenije. V prvem delu prispevka so najprej predstavljeni glavni rezultati raziskave o rabi mobilnih naprav, ogroženosti ter uporabi ustrezne zaščite, ki je bila opravljena v poslovnem sektorju med 34 slovenskimi organizacijami. Ti podatki prikazujejo dejansko stanje ogroženosti mobilnih naprav v Sloveniji in posledično možnosti uresničevanja kibernetske kriminalitete. V drugem delu prispevka kazenskopravno obravnavamo problematiko uresničitve grožnje informacijski varnosti mobilne naprave v Sloveniji; najprej na podlagi ureditve ustreznih kaznivih dejanj v *Kazenskem zakoniku* (KZ-1, 2012),[4] pozneje pa še na podlagi prikaza uradnih statističnih podatkov Policije ter Statističnega urada Republike Slovenije o procesiranju teh kaznivih dejanj. Prispevek tako celovito obravnava problematiko napadov na mobilne naprave z vseh treh vidikov: dejansko stanje, pravna ureditev in uresničevanje pravne ureditve v kazenskopravni praksi. V sklepnem delu prispevka je ponujena rešitev za izboljšanje kibernetske varnosti mobilnih naprav in s tem zmanjšanje možnosti uresničitve kibernetske kriminalitete.

2 Raba mobilnih naprav

Pri sodobnem, stalnem dostopu do podatkov imajo glavno vlogo mobilne naprave. Med uporabniki so zdaj priljubljene dokaj preproste mobilne naprave, katerih uporabnost se je v preteklih letih zelo povečala (International Data Corporation [IDC], 2012; Riedy, Beros in Wen, 2011; Smolič in Mlinar, 2001). Poročilo podjetja IDC (2014), ki prikazuje prodajo pametnih mobilnih telefonov (ti so med mobilnimi napravami), pove, da je samo v letu 2013 prodaja omenjenih naprav presegla milijardo kosov. V letu 2016 je podjetje IDC (2017) zaznalo 2,5-odstotno rast prodaje mobilnih naprav, kar je najmanj do zdaj, vendar zaradi novih naprav v letu 2017 pričakujejo ponovno rast prodaje na tri odstotke, v letu 2018 pa naj bi se ta ponovno povečala za 4,5 odstotka. Organizacije nameravajo prodajne in svetovalne oddelke opremiti s pametnimi telefoni in aplikacijami za tablične naprave. Pilotni projekti so pokazali, da mobilne aplikacije skrajšajo cikel prodaje izdelka, spreminjajo pa tudi kulturo podjetja. Po raziskavi *CEE Telco Industry Report*, ki jo je izvedla organizacija GfK Group (2011)[5], je Slovenija po uporabi pametnih mobilnih telefonov vodilna, saj kar 27,8 odstotka uporabnikov mobilne telefonije uporablja pametni mobilni telefon, sledijo ji Turčija s 23,7 odstotka in Litva z 18,5 odstotka (GfK Group, 2011). Japelj (2016) pravi, da se z razvojem tehnologije in povečanjem števila uporabnikov lahko pričakuje več zlorab kibernetskega prostora in k temu pritegne tudi storilce kaznivih dejanj.

Nekoč so ljudje komunicirali večinoma neposredno, zdaj pa se spoznavamo in pogovarjamo v kibernetskem prostoru. Spletne storitve, ki omogočajo nenehno interakcijo uporabnikov (uporaba spletnih klepetalnic, spletne pošte itn.), potrebujejo stalen dostop do prenosa podatkov. V Nemčiji so z raziskavo mladostnikov o njihovi uporabi mobilnih naprav dokazali, da je stalna komunikacija po mobilnih napravah zelo pomembna. Večina sodelujočih je izrazila močan negativen čustven odziv ob ideji, da bi dostop do interneta oziro-

[4] V prispevku niso obravnavana procesna vprašanja, ki zahtevajo samostojno obravnavo.

[5] Zajela je 15 držav Srednje in Vzhodne Evrope.

ma mobilnih naprav začasno izgubili (Vorderer, Kröemer in Scheider, 2016).

Tudi v policijski dejavnosti je raba mobilnih naprav vse pogostejša. Tako imajo patruljni policisti v 24 okrajih okrožja Montgomery v Ameriki možnost prek mobilnih naprav pridobiti informacije v realnem času. Sistem jim omogoča tudi preverjanje ljudi, pridobivanje drugih informacij in v splošnem pomoč pri delu. S tem lahko bolje in hitreje opravljajo svoje delo in tako varujejo prebivalce okrožja. Sistem zdaj deluje v 240 lokalnih in zveznih agencijah v zveznih državah Ohio in Indiana, kjer jim je v enem letu s tem sistemom uspelo zmanjšati število zaposlenih policistov s 380 na 330 (Ritchey, 2012). Tang in Xu (2012) celo opisujeta delovanje posebnega brezžičnega omrežja samo za potrebe policije in uporabo mobilnih naprav ter posebej prilagojenih aplikacij za obveščanje o incidentih, prometu idr. Goswami, Vatsa in Singh (2017) navajajo, da je uporaba mobilnih naprav pri policijskem delu zelo pomembna pri odkrivanju osumljencev, ki so jih posnele varnostne ali druge kamere. Dodajajo, da jim uporaba sistemov za avtomatsko prepoznavo obraza lahko v veliko primerih olajša delo. Za nadzor nad policijskim delom se uporabljajo kamere v avtomobilih (angl. *dashcam*) ter vedno pogosteje kamere, ki jih policisti nosijo na sebi. S tem se ne zagotovi le nadzor nad njimi kot policisti, ampak tudi pridobi dokazno gradivo v kazenskopravnih postopkih (George in Meadows, 2016).

Tudi v državah tretjega sveta se kažejo podobne smernice uporabe mobilnih naprav kot v najrazvitejših državah. Znano je, da se je v nekaj letih močno povečalo število uporabnikov mobilnih naprav v Liberiji, hkrati pa se je zelo poslabšala njihova informacijska varnost (Best, Smythe, Etherton in Wornyo, 2010; Goodman in Harris, 2010). Hitremu razvoju mobilnih naprav sledi tudi pospešen razvoj raznovrstne programske opreme zanje. Vedno več je programov, ki uporabniku olajšujejo vsakodnevna zasebna in službena opravila ter mu omogočajo lažji dostop do informacij in s tem boljšo obveščenost (Hurlburt, Voas in Miller, 2011; Weber in Darbellay, 2010). Tiongson (2015) dodaja, da je uporaba aplikacij oziroma programov za mobilne naprave del našega vsakdanjika in ima ključno vlogo pri naših odločitvah, prav tako pa je pomembna za krepitev odnosa med podjetji in njihovimi strankami.

Raba mobilnih naprav je lahko osebna, kar pomeni, da uporabnik uporablja mobilno napravo izključno za zasebne namene (vsi podatki, delovni procesi idr. so narejeni za zasebne namene), poslovna, torej za poslovne namene (podatki in delovni procesi na mobilni napravi so povezani izključno z neko organizacijo – poslovno), ali pa kombinacija osebne in poslovne rabe, torej kombinirana. To pomeni, da uporabnik eno mobilno napravo uporablja tako za osebne kot poslovne namene. Izhajajoč iz načina uporabe mobilne naprave, torej kako in s katerim namenom se ta uporablja, je ta tudi predmet različnih groženj, ki posledično lahko vodijo v kibernetsko kriminaliteto.

Grožnje lahko delujejo samostojno ali sočasno oziroma kombinirano, vedno pa z namenom, da nekdo vstopi (avtorizirano ali neavtorizirano) v informacijski sistem (Frideman in Hoffman, 2008; Loo, 2009; McAfee, 2011, 2012, 2013, 2014a, 2014b, 2015b; Vidic, 2009). Storilec lahko že s prenosom raznih sporočil (elektronska pošta ipd.) pridobi premoženjsko korist od naslovnika (Gradišar in Lamberger, 2010; Lamberger, Slak in Dobovšek, 2013). Različne grožnje so velika nevarnost za organizacije in posameznike ter ogrožajo informacijske sisteme. So raznolike in se večkrat pojavljajo sočasno, zato pri ogroženosti sistema in informacij ob sočasnem delovanju groženj uporabljamo izraz kombinirane grožnje. Ogroženi so vsi uporabniki mobilnih naprav, če pa uporabnik deluje znotraj informacijskega sistema organizacije, to pomeni, da so ogroženi tudi podatki in celoten informacijski sistem (kibernetska varnost) organizacije.

Grožnje informacijski varnosti pri uporabi mobilnih naprav niso omejene na geografsko lego in jih je geografsko nemogoče opredeliti, zato te grožnje in navajanje izrazov, ki se navezujejo nanje, uvrščamo med nadnacionalne in globalne grožnje, torej tiste, ki niso omejene z državnimi mejami (Resolucija o strategiji nacionalne varnosti Republike Slovenije, 2010).

Primer hitrorastoče grožnje mobilnim napravam je zlonamerna koda (malware, spyware, virusi, trojanski konji ipd.). V letih 2010, 2011 in 2012 so odkrili skupno 576 različic zlonamerne kode za mobilne naprave. Leta 2010 jih je bilo 80. Od tega je bil delež groženj za operacijski sistem Android le 11,25-odstoten, delež groženj za sistem Symbian, ki je bil največji, pa 62-odstoten. Konec leta 2010 se je priljubljenost sistema Android bliskovito povečala in s tem tudi delež malwara na tem operacijskem sistemu, ki je leta 2011 dosegel 66,7 odstotka od skupno 195 variacij malwara, pri Symbianu pa se je delež zmanjšal na 29,7 odstotka. Leta 2012 je od skupno 301 različice zlonamerne kode delež, ki je bil usmerjen proti sistemu Android, znašal 79 odstotkov (F-secure, 2013). Smernice povečevanja količine škodljive programske opreme so se nadaljevale tudi leta 2013, saj podjetje Juniper Networks navaja veliko povečanje groženj mobilnim napravam. Poročilo je bilo sestavljeno na podlagi enoletnega stalnega spremljanja razvoja in pojavljanja groženj mobilnim napravam. Tako se je količina škodljive programske opreme od marca 2012 do marca 2013 povečala za 614 odstotkov. Od tega kar 73 odstotkov škodljive programske opreme deluje na način iskanja varnostnih lukenj pri mobilnem plačevanju (Juniper Networks, 2013). Trendi rasti škodljive programske opreme so se nada-

ljevali tudi v letih 2014, 2015 in 2016, toda v letu 2016 (ki so ga označili kot leto izsiljevalskega virusa (tj. ransomwara)) je bila v ospredju izsiljevalska programska oprema, katere trend se je nadaljeval tudi v letu 2017. Razlog za to je naraščajoča uporaba skupnih knjižnic, saj se je s tem povečalo tudi tveganje za mobilne naprave in IoT (McAfee, 2014a, 2014b, 2015a, 2015b, 2016, 2017).

2.1 Raziskava o informacijski varnosti mobilnih naprav med slovenskimi organizacijami

2.1.1 Metoda

Raziskavo smo izvedli z uporabo spletnega vprašalnika, ki je bil od maja 2012 do februarja 2013 objavljen na spletnem portalu 1ka (www.1ka.si) (Markelj, 2014). Spletni vprašalnik je v tem času izpolnilo malo več kot 600 uporabnikov mobilnih naprav iz 34 različnih organizacij v Sloveniji. Skoraj polovica vprašalnikov je bila izpolnjena nepopolno – te smo izločili iz nadaljnje analize. Za analizo smo uporabili 309 izpolnjenih spletnih vprašalnikov, vendar tudi pri teh nekateri sodelujoči niso odgovorili na vsa vprašanja, zato smo morali vzorec prilagajati. Vsakemu vprašanju smo tako dodali informacijo o populaciji, ki je bila zajeta v vzorec.

Najprej smo želeli pridobiti nekaj osnovnih podatkov o izpraševancih, zato smo postavili vprašanje o velikosti organizacije, iz katere prihajajo. Največji odstotek ljudi, ki so odgovarjali na vprašanje, prihaja iz velikih podjetij; teh je bilo 81 odstotkov, deleži anketirancev iz preostalih velikosti podjetij pa so bili bistveno manjši. Iz mikropodjetij sta bila dva odstotka vprašanih, iz majhnih podjetij osem odstotkov in iz srednje velikih podjetij devet odstotkov vseh. Razmerje med velikostjo podjetja in tistimi, ki so odgovarjali na spletno anketo, je razumljivo. Večje je podjetje, več ljudi lahko odgovarja na anketo in posledično sta večja frekvenca in delež. V nadaljevanju smo želeli izvedeti tudi, katero stopnjo izobrazbe imajo izpraševanci.

Največ anketirancev je končalo višjo, visoko ali univerzitetno stopnjo študija (65 odstotkov), 19 odstotkov jih je imelo srednješolsko izobrazbo, 15 odstotkov pa jih je imelo magisterij ali doktorat. Glede na rezultate v tabeli lahko trdimo, da so med izpraševanci ljudje s stopnjo izobrazbe, ki jim omogoča dovolj razgledanosti in znanja, da lahko prepoznavajo grožnje rabi mobilnih naprav, vrednost posledic ob uresničitvi groženj in pomen rabe varnostnih zaščit.

2.1.2 Rezultati

Podatki iz raziskave nam pokažejo, s katero vrsto podatkov uporabniki mobilnih naprav v posameznih organizacijah delajo. Hkrati dobimo tudi podatek o načinu uporabe mobilnih naprav, njihovi zaščiti in prijavi možnih incidentov.

Tabela 1: Vrste podatkov, do katerih uporabniki dostopajo z mobilno napravo.

	N (277)	%
Osebni podatki (fotografije, elektronska pošta, sporočila idr.)	273	99
Poslovne skrivnosti (podatki, ki so znani določenemu krogu ljudi znotraj organizacije in imajo visoko tržno vrednost)	47	17
Tajni podatki (podatki, ki bi z razkritjem lahko škodovali organizaciji ter ogrozili njene gospodarske in politične koristi)	13	5

Tabela 1 prikazuje, do katerih podatkov dostopajo uporabniki mobilnih naprav. Izpraševanci so lahko hkrati izbrali več ponujenih odgovorov. Na vprašanje jih je odgovorilo 277 (100 odstotkov). Največ vprašanih dostopa do osebnih podatkov (99 odstotkov od 277 izpraševancev), kar je zanimiv podatek glede na to, da uporabljajo službeno mobilno napravo. 17 odstotkov jih dostopa do poslovnih skrivnosti in pet odstotkov do tajnih podatkov. Vsi podatki, s katerimi uporabniki delujejo prek mobilne naprave, imajo svojo vrednost in tako ob posegu v njihovo integriteto pomenijo tveganje za organizacijo. Zato je še toliko pomembneje, da se uporabniki mobilnih naprav zavedajo grožnje in da ob njeni morebitni uresničitvi znajo pravilno ravnati. S tem namenom v nadaljevanju prispevka predstavljamo odgovore na vprašanje o poznavanju oziroma zavedanju groženj uporabnikom mobilnih naprav pri rabi različnih storitev.

Pri vprašanju *Pri rabi mobilnih napravi se mi lahko zgodi* smo izpraševancem omogočili, da pri posamezni grožnji izberejo med štirimi možnostmi (1 – grožnje ne poznam; 2 – ne verjamem; 3 – verjamem; 4 – se mi je že zgodilo). Podatki iz raziskave pokažejo, da je osem odstotkov izpraševancev že doživelo odtujitev mobilne naprave, dva odstotka oddajanje podatkov brez njihove vednosti in po en odstotek jih je že doživelo krajo podatkov, sledenje (posledica nenadzorovanega oddajanja GPS-modula) ali okužbo z zlonamerno kodo (malware, spyware, virusi, trojanski konji itn.). To so seveda samo podatki za primere zaznanih groženj. Pojavlja se vprašanje, koliko je še groženj, ki jih uporabniki ne zaznajo. Glede na ravno omenjena dejstva o že zaznanih uresničenih grožnjah med uporabniki mobilnih naprav lahko trdimo, da pri rabi mobilnih naprav in uresničitvi groženj obstaja tveganje izgube podatkov, zato je zelo pomembno poznavanje stanja rabe varnostnih sredstev in ukrepov v posameznih organizacijah.

Tabela 2: Varnostni vidiki rabe mobilnih naprav

	N (274)	**%**
Preden začnem uporabljati nov model mobilne naprave, se poučim o njenih funkcijah	213	78
Za delo v podjetju uporabljam osebno mobilno napravo.	99	36
Mojo mobilno napravo uporabljajo tudi drugi.	28	10
Podatke na mobilni napravi kriptiram.	27	10
Mobilno napravo puščam vsem na očeh (lahko dostopno) na javnem mestu.	13	5
Geslo za dostop do mobilne naprave zaupam tudi drugim.	5	2

Pri vprašanju, obravnavanem v tabeli 2, smo ugotavljali varnostne vidike pri rabi mobilnih naprav med posameznimi uporabniki. Pri tem vprašanju so izpraševanci lahko hkrati izbrali več predlaganih odgovorov o rabi mobilnih naprav. Na vprašanje je odgovorilo 274 izpraševancev (100 odstotkov). Pri rabi mobilnih naprav se je meja med osebnim in poslovnim popolnoma zabrisala, kar kažejo tudi rezultati naše raziskave. Ugotovili smo, da kar 36 odstotkov od 274 izpraševancev uporablja osebno mobilno napravo tudi za poslovne namene. Spodbudno je sicer, da se jih 78 odstotkov pouči o funkcijah nove mobilne naprave, preden jo začnejo uporabljati, osupljiv pa je podatek, da jih deset odstotkov dovoli, da njihovo mobilno napravo uporabljajo tudi drugi ter da jih dva odstotka zaupa geslo za dostop do mobilne naprave tudi drugim ljudem. Če ta dejstva povežemo še z ugotovitvama, da le deset odstotkov vprašanih na mobilni napravi uporablja kriptiranje podatkov in da jih pet odstotkov pušča mobilno napravo vsem na očeh, lahko sklepamo, da deset odstotkov uporabnikov ravna zelo lahkomiselno. Puščanje mobilne naprave vsem na očeh in njeno izročanje drugim ljudem (pri čemer podatki na napravi niso kriptirani in jih z lahkoto prebere kdor koli) je zelo naivno. Pri takšnem ravnanju so možne zlorabe mobilne naprave in podatkov na njej.

V nadaljevanju smo s faktorsko analizo ugotovili povezave med spremenljivkami (ki kažejo rabo mobilnih naprav – storitev na mobilnih napravah in istočasno stopnjo ogrožanja), to pa smo pozneje uporabili pri združevanju spremenljivk v skupine. Tak način olajša statistično obdelavo spremenljivk. Faktorsko analizo smo naredili na podlagi pridobljenih odgovorov na vprašanje *Ocenitev verjetnosti zlorabe pri uporabi naštetih storitev na mobilni napravi*, na katero so izpraševanci odgovarjali z ocenami od 1 do 4 (1 = nikoli, 4 = vedno). Pričakovana razsežnost faktorske analize so faktorji, ki bodo skupni imenovalec med danimi spremenljivkami znotraj posameznega faktorja. Faktorsko analizo smo naredili po metodi glavnih osi. Posamezen faktor smo izračunali kot povprečje združenih spremenljivk.

Podatki so normalno porazdeljeni in mere asimetrije ter sploščenosti so ustrezne (vrednosti so od –3 do 3).

Tabela 3: Pri uporabi naštetih storitev so možne zlorabe – združena tabela faktorske analize in spremenljivk, ki sestavljajo faktor

Cronbachov koeficient alfa: 0,91
Metoda rotacije: varimax
Kaiser-Meyer-Olkinova mera primernosti vzorca: 0,89
Barttletov test (sig.): 0,00
Odstotek skupne pojasnjene variance: 63,14 %

F1: Raba za zasebne namene

Odstotek pojasnjene variance: 32,2
Povprečna vrednost: 2,50; standardni odklon: 0,57

	Faktorske uteži	***M***	***SD***
Prenos različnih programov z interneta	0,89	2,66	0,67
Prenos podatkov, datotek z interneta	0,85	2,64	0,65
Uporaba različnih programov za delo in razvedrilo	0,80	2,40	0,65
Shranjevanje dokumentov na spletna mesta	0,67	2,31	0,68
Dostop do spletnih socialnih omrežij	0,76	2,48	0,70

Tabela 3: Pri uporabi naštetih storitev so možne zlorabe – združena tabela faktorske analize in spremenljivk, ki sestavljajo faktor

Cronbachov koeficient alfa: 0,91 Metoda rotacije: varimax Kaiser-Meyer-Olkinova mera primernosti vzorca: 0,89 Barttletov test (sig.): 0,00 Odstotek skupne pojasnjene variance: 63,14 %			
F1: Raba za zasebne namene			
Odstotek pojasnjene variance: 32,2 Povprečna vrednost: 2,50; standardni odklon: 0,57			
	Faktorske uteži	***M***	***SD***
Prenos različnih programov z interneta	0,89	2,66	0,67
Prenos podatkov, datotek z interneta	0,85	2,64	0,65
Uporaba različnih programov za delo in razvedrilo	0,80	2,40	0,65
Shranjevanje dokumentov na spletna mesta	0,67	2,31	0,68
Dostop do spletnih socialnih omrežij	0,76	2,48	0,70
F2: Raba za službene namene			
Odstotek pojasnjene variance: 31,0			
Povprečna vrednost: 2,24; standardni odklon: 0,47			
	Faktorske uteži	***M***	***SD***
Povezava na poslovni sistem organizacije	0,81	2,01	0,64
Prenos elektronske pošte	0,59	2,36	0,63
Brskanje po spletu	0,50	2,53	0,58
Spletno nakupovanje	0,59	2,35	0,61
E-bančništvo	0,78	2,11	0,63
Izmenjava poslovnih podatkov	0,76	2,27	0,61
Opravljanje službenih obveznosti na delovnem mestu	0,73	2,03	0,63

V faktorski analizi smo ocenjevali zavedanje verjetnosti zlorabe pri rabi različnih storitev na mobilnih napravah. V prvem koraku smo izvedli faktorsko analizo, s katero smo spremenljivke razvrstili na dva faktorja s pravokotno rotacijo (varimax z normalizacijo Kaiser). V kateri faktor spada posamezna spremenljivka, smo določili glede na faktorsko utež posamezne spremenljivke ter korelacijo posamezne spremenljivke glede na posamezen faktor. Na podlagi odstotka pojasnjene variance (nad 60 odstotki) in velikosti faktorske uteži (nad 0,5) zagotavljamo, da je faktorska analiza ustrezna. Spremenljivke smo tako na podlagi rezultatov faktorske analize razdelili v dve skupini oziroma dva faktorja. Prvi faktor smo poimenovali *raba za zasebne namene*. Na podlagi faktorske analize smo vanj uvrstili spremenljivke, ki si sledijo glede na korelacijo (utež) posamezne spremenljivke in faktorja: prenos programov z interneta, prenos podatkov z interneta, uporaba različnih programov za delo in razvedrilo, dostop do spletnih socialnih omrežij ter shranjevanje dokumentov na spletna mesta. V drugi faktor, ki smo ga poimenovali *raba za službene namene*, smo uvrstili spremenljivke, ki si sledijo glede na korelacijo (utež) posamezne spremenljivke in faktorja: zloraba mobilne naprave pri povezavi na poslovni informacijski sistem organizacije, uporaba e-bančništva in izmenjava poslovnih podatkov.

Koeficient zanesljivosti (Cronbachov koeficient alfa) je pri omenjeni faktorski analizi 0,91, kar pomeni visoko stopnjo zanesljivosti tega sklopa vprašanj, medtem ko je skupna varianca 63,14 odstotka. Podatki so normalno porazdeljeni.

V drugem koraku smo na podlagi rezultatov faktorske analize ustvarili dva indeksa[6] (tabela 4) in nato naredili t-test indeksov uporabe mobilnih storitev (tabela 5). Povprečje in standardni odlok posameznega indeksa smo izračunali na podlagi spremenljivk, ki smo jih uvrstili v posamezen indeks. Za namene izpeljave t-testa indeksov smo določili mejno vrednost indeksov, ki je v tem primeru 2, potem smo izračunali razliko med povprečno in mejno vrednostjo (Mean Difference) (tabela 6) ter p-vrednost posameznih indeksov. Povprečje pri obeh indeksih je statistično značilno večje od 2.

Tabela 4: Povprečje izbranih spremenljivk – indeks

	N	*M*
Indeks rabe mobilnih storitev za zasebne namene	296	2,49
Indeks rabe mobilnih storitev za službene namene	283	2,24

Iz tabele opisne statistike (tabela 5) je razvidno, da je povprečje pri obeh spremenljivkah nad 2. Ali je ta razlika statistično značilna, pokaže t-test.

Ker je p-vrednost testa pod 0,05, lahko zavrnemo ničelno hipotezo, ki pravi, da je povprečje enako 2, in sprejmemo nasprotno: povprečje je večje od 2. Sklepamo lahko, da je pri uporabi storitev za zasebne in poslovne namene na mobilnih napravah zavedanje o ogroženosti pogosto. Vrednost (p-vrednost) pri obeh indeksih je manjša od 0,05, kar pomeni, da sta oba indeksa statistično značilna glede na našo mejno vrednost. To pomeni, da je pri uporabi mobilnih naprav pri obeh indeksih zavedanje o ogroženosti pogosto.

Tabela 5: T-test indeksov

	Mejna vrednost = 2			***Razlika v aritmetičnih sredinah***
	t	***df***	***p***	
Indeks uporabe mobilnih storitev za zasebne namene	8,81	30	,00	,24
Indeks uporabe mobilnih storitev za službene namene	14,78	28	,00	,49

Predstavljeni rezultati raziskave pokažejo, da je zavedanje o ogroženosti pri rabi mobilnih naprav in omenjenih storitev pogosto (tako pri zasebni kot poslovni rabi). Hkrati je iz rezultatov razvidno, da se uporabniki mobilnih naprav zavedno izpostavljajo grožnjam (posojanje mobilnih naprav drugim, nekriptiranje podatkov ter mešanje osebnih in poslovnih podatkov) in s tem povečujejo možnosti uresničitve kibernetske kriminalitete.

3 Kazenskopravni vidiki informacijske varnosti mobilnih naprav

3.1 Ureditev v *Kazenskem zakoniku* (KZ-1, 2012)

Po predstavitvi dejanskega stanja rabe in ogroženosti mobilnih naprav v Sloveniji bomo predstavili še zakonsko podlago za kazenskopravno obravnavanje ogrožanja informacijske varnosti mobilnih naprav. Uresničena grožnja informacijski varnosti mobilne naprave je namreč lahko tudi kaznivo dejanje, ustrezne definicije kaznivih dejanj pa moramo opredeliti tudi zato, da bomo v nadaljevanju lahko preverili, kako organi kazenskega pregona in pravosodja procesirajo napade na mobilne naprave v praksi.

V Sloveniji ne poznamo kaznivih dejanj, ki bi posebej (kot *lex specialis*) inkriminirala napade na mobilne naprave, ampak je v zvezi s tem treba uporabiti splošnejša kazniva dejanja, ki jih v Sloveniji v teoriji in tudi praksi (npr. letna poročila policije ali državnega tožilstva) poznamo pod imenom računalniška[7] ali kibernetska (Svet Evrope, 2004) kriminaliteta. V zvezi s tem je treba najprej odgovoriti na vprašanje, ali mobilno napravo lahko štejemo za informacijski sistem, saj nekatera kazniva dejanja iz KZ-1 (2012) vsebujejo informacijski sistem kot zakonski znak kaznivega dejanja. *Direktiva Evropske unije (EU) o napadih na informacijske sisteme* (2013) tako opredeljuje informacijski sistem kot »*napravo ali skupino med seboj povezanih ali sorodnih naprav, od katerih ena ali več ob uporabi programa opravlja samodejno obdelavo računalniških podatkov, kakor tudi računalniške podatke, ki so shranjeni, obdelani, pridobljeni ali se po tej napravi ali skupini naprav prenašajo zaradi njenega ali njihovega delovanja, uporabe, varovanja in vzdrževanja*«.[8] Glede na to, da sta dve najpomembnejši strukturi mobilne naprave prav programska (angl. *app*) in strojna oprema (Markelj, 2014), mobilna naprava ustreza opredelitvi informacijskega sistema.

Upoštevajoč sistematiko *Direktive EU o napadih na informacijske sisteme* (2013)[9], slovenski KZ-1 (2012) pozna tri

[6] Imenujeta se enako kot faktorja z dodatkom *indeks*.

[7] Tak izraz uporablja policija, a je preozek (Završnik, 2005: 249).

[8] *Konvencija Sveta Evrope o kibernetski kriminaliteti* (2004) sicer uporablja izraz računalniški sistem, a ta vsebinsko ustreza definiciji direktive EU.

[9] Direktiva EU o napadih na informacijske sisteme (2013) ureja naslednja kazniva dejanja: nezakonit dostop do informacijskih sistemov, nezakonito poseganje v sistem, nezakonito poseganje v podatke, nezakonito prestrezanje in orodja, ki se uporabljajo za izvedbo kaznivih dejanj.

upoštevna kazniva dejanja, pri katerih je predmet napada informacijski sistem: napad na informacijski sistem (221. člen), zloraba informacijskega sistema (237. člen) ter izdelovanje in pridobivanje orožja in pripomočkov, namenjenih za kaznivo dejanje (306. člen).[10]

Napad na informacijski sistem je kaznivo dejanje zoper premoženje, stori pa ga vsakdo, ki neupravičeno vstopi ali vdre v informacijski sistem ali neupravičeno prestreže podatek ob nejavnem prenosu v informacijski sistem ali iz njega. Za kvalificirano obliko tega kaznivega dejanja gre v primeru, ko nekdo podatke v informacijskem sistemu neupravičeno uporabi, spremeni, preslika, prenaša ali uniči oziroma v informacijski sistem neupravičeno vnese kakšen podatek, ovira prenos podatkov ali delovanje informacijskega sistema, pa tudi v primeru, ko je z dejanjem povzročena velika škoda.[11] S tako opredelitvijo kaznivega dejanja slovenska ureditev skoraj popolnoma ustreza definicijam kaznivih dejanj iz omenjene direktive EU (Direktiva EU o napadih na informacijske sisteme, 2013), neurejeno je le še izvršitveno ravnanje prestrezanja s tehničnimi sredstvi nejavnega prenosa podatkov *znotraj* informacijskega sistema. V tem delu torej omenjena direktiva še ni implementirana. Omeniti je treba tudi, da uporaba zakonskega znaka *informacijski sistem* kaže, da je kazenska zakonodaja upoštevala tehnološki razvoj, saj sta prvotni definiciji tega kaznivega dejanja iz *Kazenskega zakonika* (KZ, 2004) govorili le o podatku ali programu, namenjenem za računalniško uporabo ali obdelavo oziroma zaščiteno računalniško bazo podatkov (KZ-A, 1999). Že na prvi pogled je jasno, da sta ti dve opredelitvi z današnjega vidika preozki, saj poleg računalniškega poznamo še druge informacijske sisteme, med drugim mobilne naprave. Poleg tega Bernik in Meško (2011) navajata, da je pri analiziranju kaznivega dejanja poleg vidika storilca, žrtve in okoliščin kaznivega dejanja treba upoštevati tudi strah pred kriminaliteto, ki vpliva na zaznavanje negativnih pojavov in odzivanje ljudi nanje.

Lex specialis kaznivo dejanje zlorabe informacijskega sistema iz 237. člena KZ-1 (2012) je kaznivo dejanje zoper gospodarstvo (Deisinger, 2002: 510), ki ga stori tisti, ki pri gospodarskem poslovanju neupravičeno vstopi ali vdre v informacijski sistem ali ga neupravičeno uporablja tako, da uporabi, spremeni, preslika, prenaša, uniči ali v informacijski sistem vnese kakšen podatek, ovira prenos podatkov ali delovanje informacijskega sistema ali neupravičeno prestreže podatek ob nejavnem prenosu v informacijski sistem, da bi sebi ali komu drugemu pridobil protipravno premoženjsko korist ali drugemu povzročil premoženjsko škodo (KZ-1, 2012: 237. člen). Gre za kaznivo dejanje t. i. gospodarske špijonaže, ki je v nasprotju s kaznivim dejanjem iz 221. člena KZ-1 (2012) lahko storjeno le pri opravljanju gospodarske dejavnosti.

V skladu s 306. členom KZ-1 (2012) je inkriminiran tudi vsakdo, ki z namenom storitve kaznivega dejanja poseduje, izdeluje, prodaja, daje v uporabo, uvaža, izvaža ali kako drugače zagotavlja pripomočke za vdor ali neupravičen vstop v informacijski sistem. Tudi s to inkriminacijo Slovenija že zdaj primerno izpolnjuje zahtevo iz omenjene direktive EU. Ta člen kot samostojno kaznivo dejanje (*delictum sui generis*) opredeljuje nekatera ravnanja, ki so po svojih značilnostih dejanja pomoči pri kaznivem dejanju vdora ali neupravičenega vstopa v informacijski sistem. Če storilec stori kaznivo dejanje iz 306. člena KZ-1 (2012), hkrati pa vsaj še poskusi vdreti ali neupravičeno vstopiti v informacijski sistem s temi pripomočki (KZ-1, 2012: 221. člen), pride do navideznega steka in odgovarja le za kaznivo dejanje po 221. členu KZ-1 (2012). Zakonodajalec je v tem členu uporabil nedovršne glagole, kar kaže na to, da za izvedbo tega kaznivega dejanja v skladu z načelom zakonitosti iz 28. člena Ustave Republike Slovenije (1991) ne zadošča enkratno posamezno ravnanje.

Če upoštevamo širšo sistematiko Konvencije Sveta Evrope o kibernetski kriminaliteti (2004) in letnih poročil policije, je treba pri kibernetski kriminaliteti omeniti še druga kazniva dejanja, pri katerih informacijski sistem ni nujno element definicije kaznivega dejanja, gre pa za kazniva dejanja *lex generalis*, ki jih je mogoče tipično izvesti tudi prek informacijskega sistema ali z njegovo uporabo, npr. kaznivo dejanje zlorabe osebnih podatkov, kršitve materialnih avtorskih pravic, izsiljevanja, terorizma,[12] izdaje in neupravičene pridobitve poslovne skrivnosti, izdaje tajnih podatkov, prikazovanja, izdelave, posesti in posredovanja pornografskega gradiva itd., odvisno od storilčevega motiva in predmeta napada.[13]

[10] Zakon o spremembah in dopolnitvah kazenskega zakonika – KZ-1E (2017) je sicer določil dve novi samostojni izvršitveni ravnanji terorizma po 108. členu, in sicer neupravičeno poseganje v informacijski sistem, ki pomeni resno oviranje ali prekinjanje njegovega delovanja z vnosom, prenosom, poškodovanjem, brisanjem ali spreminjanjem podatkov ali pa preprečevanjem ali onemogočanjem dostopa do njih in ki povzroči resno škodo ali je bilo storjeno z uporabo računalniškega programa, gesel ali kod za dostop, zasnovanih ali prilagojenih za namene storitve dejanja, ali neupravičeno poseganje v informacijski sistem kritične infrastrukture, ki pomeni resno oviranje ali prekinjanje njegovega delovanja z vnosom, prenosom, poškodovanjem, brisanjem ali spreminjanjem podatkov ali pa preprečevanjem ali onemogočanjem dostopa do njih, ter neupravičeno brisanje, poškodovanje ali spreminjanje podatkov v informacijskem sistemu kritične infrastrukture ali pa preprečevanje ali onemogočanje dostopa do takih podatkov. A ker KZ-1E (2017) velja od 2. julija 2017, podatkov o njegovi uporabi seveda še ni, zato to kaznivo dejanje ni bilo zajeto v statistični pregled.

[11] 221. člen KZ-1 (2012). V skladu z 99. členom KZ-1 (2012) velika škoda pomeni škodo, večjo od 50.000 evrov.

[12] Glej opombo št. 10.

[13] Glej denimo 143., 148., 213., 108., 236., 260. in 176. člen KZ-1 (2012).

3.2 Kibernetska kriminaliteta v slovenski kazensko-pravni praksi

Slovenska kazenska zakonodaja (z manjšimi izjemami) pozna primerne definicije kaznivih dejanj, ki bi zajele tudi napade na mobilne naprave, še posebno z inkriminacijami računalniške kriminalitete, ki v skladu z letnimi poročili policije vsebuje naslednja kazniva dejanja: zloraba osebnih podatkov, zloraba informacijskega sistema, kršitev materialnih avtorskih pravic na internetu, napad na informacijski sistem ter izdelovanje in pridobivanje orožja in pripomočkov, namenjenih za kaznivo dejanje. Vprašanje pa je, kako se te določbe uresničujejo v praksi.

V nadaljevanju bomo zato predstavili podatke o zaznanih kaznivih dejanjih, ovadenih osumljencih in obsojenih osebah v letih 2006–2015, ki bodo pokazali dejansko stanje uporabe teh kazenskopravnih določb.[14]

lje kriminalitete (Bavcon, Šelih, Ambrož, Filipčič in Korošec, 2013: 38), ker se za prijavljanje tovrstnih kaznivih dejanj odloči redko katera organizacija ali posameznik (Lukan, 2009). Ti podatki predstavljajo fazo predkazenskega postopka, ko obstaja le najnižji dokazni standard (razlogi za sum), da je bilo storjeno kaznivo dejanje – lahko ga je storil tudi neznani storilec, in ko je kaznivo dejanje šele zaznano, vendar je število odvisno predvsem od prijavljanja teh dejanj (Lukan, 2009; Kolenc, Kebe in Bukovnik, 2013). Število zaznanih kaznivih dejanj zlorabe osebnih podatkov se tako od leta 2009 zmanjšuje, z izjemo leta 2014; število zaznanih zlorab informacijskega sistema se je povečevalo do leta 2011, nato se je začelo zmanjševati, v letih 2015 in 2016 pa je spet mogoče zaznati večje število teh kaznivih dejanj. Število zaznanih kršitev avtorskih pravic na internetu se je zmanjševalo do leta 2012, nato pa se je začelo povečevati. Za število zaznanih kaznivih dejanj napadov na informacijski sistem in izdelavo

Tabela 6: Število zaznanih kaznivih dejanj (vir: Policija, 2007–2016)

Leto	Zloraba osebnih podatkov[15]	Zloraba informacijskega sistema	Kršitev materialnih avtorskih pravic na internetu	Napad na informacijski sistem	Pripomočki, namenjeni za kaznivo dejanje
2006	ni podatka	6	6	24	2
2007	ni podatka	4	7	88	13
2008	ni podatka	7	10	283	10
2009	11[16]		5	98	0
2010	3	15	5	76	2
2011	5	26	3	236	6
2012	3	12	2	131	3
2013	2	8	6	226	2
2014	5	1	1	155	6
2015	3	6	2	162	1
2016	1	10	4	260	3

Tabela 6 kaže število zaznanih kaznivih dejanj na podlagi letnih poročil policije. Te številke so pričakovano nižje od podatkov o dejanski ogroženosti mobilnih naprav, saj je tudi v zvezi s temi kaznivimi dejanji treba upoštevati temno pripomočkov velja, da ni mogoče zaznati enotnega trenda, mogoče pa je ugotoviti, da je izmed vseh omenjenih kaznivih dejanj največ zaznanih prav napadov na informacijski sistem; prvi vrhunec zaznav teh kaznivih dejanj je mogoče zaznati v letih 2007–2008, drugega pa v letu 2011. V preostalih letih je mogoče zaznati padec. Policija kot razlog za povečanje zaznanih kaznivih dejanj navaja povečano, a premalo varno rabo elektronskih naprav.[17]

[14] Seveda se ti podatki nanašajo na vse informacijske sisteme, ne le na mobilne naprave.

[15] Kazniva dejanja zajemajo vse različice teh kaznivih dejanj iz KZ (2004) in KZ-1 (2012); 154., 159., 225., 242. in 309. člen KZ (2004) ter 143., 148., 221., 237. in 306. člen KZ-1 (2012).

[16] V tem letu je bil zapisan skupen podatek za zlorabo osebnih podatkov ter informacijskega sistema.

[17] Npr. Poročilo o delu policije za leto 2013 (Policija, 2014: 23).

Tabela 7: Število ovadenih osumljencev (vir: Policija, 2007–2016)

Leto	Zloraba osebnih podatkov[18]	Zloraba informacijskega sistema	Kršitev materialnih avtorskih pravic na internetu	Napad na informacijski sistem	Pripomočki, namenjeni za kaznivo dejanje
2006	ni podatka	2	5	10	2
2007	ni podatka	4	6	69	17
2008	ni podatka	5	13	275	11
2009	6[19]		6	78	0
2010	3	1	7	25	3
2011	2	21	4	184	6
2012	2	4	3	45	3
2013	3	3	13	125	1
2014	0	0	15	68	6
2015	2	1	4	76	1
2016	1	5	4	117	2

Tabela 7 kaže število ovadenih osumljencev za kazniva dejanja. Te številke so še manjše, saj gre za osumljence, za katere je policija podala kazensko ovadbo državnemu tožilstvu, ker je bila prepričana, da zoper njih obstaja utemeljen sum, kar pomeni že več kot 50-odstotno verjetnost, da je prav točno določena oseba storila določeno kaznivo dejanje (Šugman, 2007: 247). Število ovadenih osumljencev za zlorabo osebnih podatkov se je rahlo povečalo, v zadnjih dveh letih pa padlo na nič; za zlorabo informacijskega sistema se zmanjšuje od leta 2011, za kršitev materialnih avtorskih pravic na internetu pa se povečuje od leta 2011. Za število ovadenih osumljencev kaznivih dejanj napadov na informacijski sistem in izdelave pripomočkov za kaznivo dejanje velja enako kot pri zaznanih kaznivih dejanjih: prvi vrhunec je mogoče zaznati v letu 2007–2008, drugega pa v letu 2011 z vmesnim padcem.[20]

Tabela 8: Število obsojencev (vir: Statistični urad Republike Slovenije, 2015)

Leto	Napad na informacijski sistem[21]	Zloraba informacijskega sistema	Zloraba osebnih podatkov	Pripomočki, namenjeni za kaznivo dejanje
2006	1	0	1	0
2007	0	1	3	0
2008	6	0	3	6
2009	2	0	4	4
2010	7	0	3	2
2011	1	0	9	0
2012	9	0	12	1
2013	1	12	13	0
2014	8	1	25	2
2015	0	0	3	0

[18] Tudi tukaj kazniva dejanja zajemajo vse različice teh kaznivih dejanj iz KZ (2004) in KZ-1 (2012).

[19] V tem letu je bil zapisan skupen podatek za zlorabo osebnih podatkov ter informacijskega sistema.

[20] Tudi razlog za to naj bi bil enak: povečana in premalo varna raba elektronskih naprav.

[21] Tudi tukaj kazniva dejanja zajemajo vse različice teh kaznivih dejanj iz KZ (2014) in KZ-1 (2012), razen pri kaznivem dejanju

Tabela 8 prikazuje število obsojencev za bistvena kazniva dejanja, pri katerih je bila krivda za kaznivo dejanje dokazana do stopnje prepričanosti (Šugman, 2007: 249). Podatki so zajeti iz baze Statističnega urada Republike Slovenije in kažejo, da je število, obsojenih za kaznivo dejanje napada na informacijski sistem, nihalo. Največ obsodb najdemo v letih 2008, 2010 ter 2012, v vmesnih letih pa padce. Število, obsojenih za zlorabo osebnih podatkov, se povečuje (razen v letu 2015).

4 Razprava

Pregled slovenske in svetovne teoretične ter raziskovalne literature o rabi mobilnih naprav in informacijski varnosti pokaže, da se raba mobilnih naprav v zadnjih letih drastično povečuje. Mobilne naprave zamenjujejo osebne računalnike skoraj na vseh področjih posameznikovega delovanja, in to tako na osebni kot poslovni ravni. Integracija sistemov, ki delujejo na mobilnih napravah, poteka danes na vseh ravneh tehnologije (avtomobili, pametni domovi, pametna mesta, internet stvari itn.). Hkrati z razvojem mobilnih naprav in z njimi povezane tehnologije (programska oprema, omrežja itd.) se razvijajo tudi grožnje, ki poskušajo na različne načine posegati v integriteto posameznikove mobilne naprave, podatkov in posledično tudi celotnega informacijskega sistema, do katerega ima mobilna naprava dostop. Kot kaže naša raziskava med slovenskimi podjetji, se je meja med zasebno in poslovno rabo s prihodom mobilnih naprav zabrisala. Uporabnik na mobilni napravi shranjuje različne vrste podatkov, zato ob njeni uporabi obstaja tudi različna stopnja tveganja odtujitve podatkov. Ta je odvisna predvsem od načina rabe mobilne naprave, uporabe varnostnih zaščit in zavedanja groženj, ki obstajajo. Ob primeru uresničitve grožnje je treba obvestiti ustrezne organe, ki poskrbijo za zavarovanje dokazov in nadaljnjo preiskavo, saj ima uresničitev grožnje lahko tudi zakonske znake kaznivega dejanja.

S tem namenom smo v drugem delu prispevka predstavili ureditev najbistvenejših kaznivih dejanj v slovenski zakonodaji, ki so lahko podlaga za kazenskopravno ukrepanje. Ker nekatera kazniva dejanja vsebujejo zakonski znak *informacijski sistem*, je njihova uporaba odvisna od predhodnega sklepa, da je mobilna naprava informacijski sistem, lahko pa tudi del informacijskega sistema neke organizacije. Pri drugih kaznivih dejanjih taka ugotovitev ni nujna, saj gre za splošnejša kazniva dejanja, pri katerih je lahko tudi mobilna naprava predmet napada ali sredstvo dejanja, denimo neupravičeno razkritje ali dostop do nekaterih zaščitenih podatkov. Taki podatki so zaščiteni glede na svojo vsebino in ne glede na to, na katerem mediju so, torej tudi na mobilni napravi.

Pregled kazenskopravne ureditve in prakse tako kaže, da ima Slovenija trenutno tehnološkemu napredku ter mednarodnim obveznostim prilagojene definicije kaznivih dejanj, ki lahko zajamejo tudi uresničitev grožnje informacijski varnosti mobilne naprave. Praksa kazenskega pravosodja kaže, da je vedno več tovrstnih kaznivih dejanj zaznanih, procesiranih, pa tudi dokazanih, o čemer je mogoče sklepati iz števila pravnomočnih obsodilnih sodb, kljub nepojasnjenim nihanjem v nekaterih letih.

Če želijo organizacije zvišati raven kibernetske varnosti pri rabi mobilnih naprav in s tem zmanjšati tveganje uresničitve kibernetske kriminalitete, njene škode in posledično tudi svoje vpletenosti v kazenski postopek, morajo poskrbeti tako za tehnične kot tudi za organizacijske ukrepe. Z drugimi besedami: poznati in uporabljati morajo tehnične rešitve in izvajati organizacijske ukrepe. Ukrepe za varovanje mobilne naprave, podatkov in informacijskega sistema organizacije namreč delimo na dva dela: tehnični in organizacijski (netehnični). V tehnični del spadajo vse programske in strojne rešitve, ki kakor koli zavarujejo mobilno napravo in podatke. Med organizacijske rešitve pa spadajo vse tiste, ki pripomorejo k varnosti mobilne naprave in podatkov z navodili za uporabo mobilnih naprav in pripadajoče programske opreme (npr. navodila za internetno povezovanje v informacijski sistem organizacije). V organizacijski del rešitev uvrstimo vse politike in standarde, ki kakor koli pripomorejo k vzpostavitvi boljše informacijske varnosti ter zavarovanju mobilne naprave in podatkov. Organizacijski del rešitev lahko imenujemo tudi *ukrepi*, ki jih organizacije sprejmejo in usvojijo za zagotovitev višje stopnje informacijske varnosti pri rabi mobilnih naprav. Rešitve za vzpostavitev informacijske varnosti pri rabi mobilnih naprav delimo na:

– tehnične rešitve;
– organizacijske rešitve in ukrepe: izobraževanja in ozaveščanja, pravilniki, standardi;
– kombinacijo tehničnih in organizacijskih rešitev ter ukrepov.

Vpeljava mobilnih naprav v organizacijsko okolje je kompleksna zadeva, če hkrati želimo poskrbeti tudi za zadostno stopnjo informacijske varnosti. Pomembno je, da z vsemi varnostnimi rešitvami in ukrepi ne izničimo vseh pozitivnih (tudi ekonomskih) učinkov, ki jih mobilne naprave prinesejo v delovno okolje. Markelj (2014) v svoji doktorski disertaciji razvije model, ki ponazarja vpeljavo mobilnih naprav v organizacijsko okolje, upoštevajoč elemente informacijske varnosti, raznolikosti in potreb delovnih procesov. Namen predsta-

zlorabe informacijskega sistema, pri katerem so bili v bazi Statističnega urada Republike Slovenije dosegljivi le podatki po 242. členu KZ (2004), ne pa tudi po 237. členu KZ-1 (2012). V tem delu so torej podatki pomanjkljivi.

vljenega modela je uvedba mobilnih naprav v organizacijsko okolje, kjer z njim (oziroma posameznimi koraki v modelu) poskrbimo za okolje, v katerem se zagotavlja ustrezna stopnja informacijske varnosti. Ima torej primerljivo oziroma podobno vlogo kot prva (primarna) skupina pri modelu prevencije kriminalitete (Meško, 2002), in sicer preprečevanje uresničitve groženj informacijski varnosti pri rabi mobilnih naprav z načrtovanjem organizacijskega okolja, ki vključuje in predvideva varno rabo mobilnih naprav.

Model omogoča varno uvedbo rabe mobilnih naprav v katero koli organizacijo. Pomembno vodilo pri njegovem oblikovanju je bilo vključevanje vseh deležnikov; uporabnike, ki jih raba mobilnih naprav v organizaciji kakor koli zadeva, je treba vključiti v uvajanje mobilnih naprav v organizacijsko okolje, med tem procesom pa tudi seznanjati s posledičnimi spremembami dela in izobraževati o njih. Model pri uvajanju mobilnih naprav v organizacijo predvideva predhodno poskusno okolje, v katerem organizacija na poskusni skupini uporabnikov preizkusi uvedbo mobilnih naprav. Organizacija tako lahko predhodno ugotovi morebitne vrzeli in jih odpravi še pred uvedbo mobilnih naprav v celotno organizacijo. Model predvideva tudi posamične korake uvedbe, da bi se lahko hkrati upoštevali načini zagotavljanja informacijske varnosti, neovirano delovanje procesov organizacije ter tudi obveščanje in izobraževanje uporabnikov o novostih. S tako potjo uvedbe mobilnih naprav v organizacijsko okolje, kot jo predvideva predstavljeni model, je zmanjšana verjetnost uresničitve katere od groženj informacijski varnosti organizacije in posledično uresničitve katere od posledic (npr. prekinitev poslovanja) zaradi sprotnega poskusnega izobraževanja uporabnikov in sodelovanja predstavnikov različnih procesov v organizaciji pri uvajanju mobilnih naprav v njeno delo.

Prvi korak uvedbe mobilnih naprav v organizacijo je prepoznavanje potreb po rabi mobilnih naprav v delovnih procesih organizacije. Organizacija mora narediti temeljito analizo, ali njeni zaposleni pri delu res potrebujejo mobilne naprave in ali je nujno, da z njimi dostopajo do poslovnih podatkov.

Drugi korak je opredelitev organizacijske strukture, podatkov in poslovnih procesov, ki se jih bo dotaknila uvedba mobilnih naprav v poslovni sistem organizacije. Uvedba mobilnih naprav v poslovne procese organizacije, njeno strukturo in informacijski sistem ne sme biti stvar posameznika ali nekega oddelka, ampak celotne organizacije in njenih procesov. Zato je treba glede na ugotovitev potreb rabe mobilnih naprav v organizaciji zagotoviti procese, storitve, ljudi in vso infrastrukturo organizacije, ki se jih bo uvedba mobilnih naprav tako ali drugače dotaknila, in njihove predstavnike povabiti v delovno skupino za uvedbo mobilnih naprav v organizacijo.

Tretji korak je oblikovanje delovne skupine, ki bo poskrbela za celovito vključitev mobilnih naprav v celoten organizacijski model organizacije in bo pri tem upoštevala informacijskovarnostne standarde. Delovno skupino morajo sestavljati ustrezno strokovno usposobljeni ljudje, ki dobro poznajo delovanje organizacije, celovito delovanje mobilnih naprav in informacijskovarnostno področje.

Četrti korak je preračunavanje stroškov uvedbe mobilnih naprav v organizacijo, tudi z upoštevanjem različnih možnosti njene izvedbe. Organizacija mora sprejeti odločitev, ali bo sama kupila mobilne naprave ali bodo zaposleni uporabljali svoje lastne (»Prinesi svojo napravo.«).

Peti korak je oblikovanje standardov, pravilnikov in navodil, ki so pravno zavezujoči in opredeljujejo tudi kazni za kršitve. Sledita izobraževanje in ozaveščanje uporabnikov o sprejetih standardih, pravilnikih in navodilih. Uporabniki mobilnih naprav morajo biti namreč seznanjeni z vsemi smernicami rabe mobilnih naprav v svoji organizaciji, saj lahko le tako delujejo v skladu s pravilniki in standardi na tem področju.

Šesti korak je pilotna uvedba mobilnih naprav v organizacijo. Glede na njene rezultate se naredi revizija vseh predhodnih korakov. Pilotna uvedba mobilnih naprav v organizacijo prikaže realno podobo rabe mobilnih naprav v neki organizaciji v določenem času. Na podlagi ugotovitev se izvede revizija vseh predhodnih korakov in ugotovi njihova uspešnost oziroma pomanjkljivosti.

Sedmi korak je dejanska uvedba, ki se začne z izobraževanjem in ozaveščanjem zaposlenih.

Hkrati pa je, kot smo že velikokrat omenili, največ odvisno od vsakega uporabnika mobilne naprave, zato je pomembno, da ta, poleg že omenjenih korakov, ki so naloga organizacije, naredi vse za varno rabo mobilne naprave ter podatkov, do katerih dostopa prek nje.

Pomembno je, da se uporabniki (tudi tisti, ki mobilno napravo uporabljajo le zasebno) zavedajo odgovornosti, ki jo prevzemajo, ko uporabljajo mobilne naprave in podatke, shranjene na njih. Uporabnikom in seveda tudi organizacijam bi bilo treba nazorno predstaviti grožnje mobilnim napravam in njihove posledice ter jih opozoriti predvsem na tiste, zaradi katerih lahko uporabnik in/ali organizacija odgovarja kazensko, disciplinsko ali odškodninsko.

5 Sklep

Povečanje rabe mobilnih naprav in z njimi povezanih sistemov se bo nadaljevalo tudi v prihodnje, hkrati s tem pa se bodo širili tudi načini rabe. Nesmiselno je razmišljati, da bi se v tem trenutku trendi načina rabe mobilnih naprav lahko tako spremenili, da bi lahko govorili o uporabnikovem razlikovanju zasebne in poslovne rabe podatkov na mobilni napravi. Zato je še toliko pomembneje zagotoviti tehnične in organizacijske rešitve, ki omogočajo zaščito podatkov pri uporabnikovem delu z mobilno napravo in posredno preprečujejo tudi škodljive posledice kršitev dela z mobilno napravo, ki so inkriminirane v obliki kaznivih dejanj. Uvajanje standardov in pravilnikov o rabi mobilnih naprav ter dostopanju do poslovnega informacijskega sistema bi tako moralo postati stalna praksa vseh organizacij.

Raba mobilne naprave v nasprotju s pravili organizacije in splošnejšimi zakonskimi zahtevami lahko povzroči tudi (kazensko)pravne posledice. V skladu s KZ-1 (2012) je sicer za obravnavana kazniva dejanja zoper informacijski sistem mogoče kazenskopravno odgovarjati le, če so storjena naklepno, toda ob upoštevanju tanke meje med morebitnim naklepom in zavestno malomarnostjo je lahko v takem primeru poleg prekrškovne in civilne pomembna tudi kazenska odgovornost. Te posledice pa je mogoče preprečiti ali odpraviti z različnimi tehničnimi rešitvami ter z uveljavitvijo pravilnikov in standardov. Najboljša informacijskovarnostna rešitev bi bila kombinacija obojega, torej tehničnih oziroma programskih rešitev internih pravilnikov in standardov, ki jasno opredeljujejo načela varne rabe mobilnih naprav, programske opreme zanje in podatkov, s katerimi delujejo posamezniki in organizacija.

Ob upoštevanju navedenih varnostnih rešitev in ukrepov bi se izboljšala tudi raven kibernetske varnosti, kar bi posledično vplivalo na obseg kibernetske kriminalitete in število kazenskih postopkov.

Literatura

1. Bavcon, L. Šelih, A., Ambrož, M., Filipčič, K. in Korošec, D. (2013). *Kazensko pravo, splošni del*. Ljubljana: Uradni list RS.
2. 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.
3. Best, M. L., Smythe, T. N., Etherton, J. in Wornyo, E. (2010). Users of mobile phones in post-conflict Liberia. *Informational Technologies & International Development, 6*(2), 91–108.
4. Deisinger, M. (2002). *Kazenski zakonik s komentarjem*. Ljubljana: GV založba.
5. Dimc, M. in Dobovšek, B. (2010). Perception of cybercrime in Slovenia. *Varstvoslovje*, *12*(4), 378–396.
6. Direktiva Evropske unije (EU) o napadih na informacijske sisteme (2013). *Uradni list EU,* (L 218).
7. Europol. (2013). *SOCTA 2013: EU serious and organised crime threat assessment*. Haag: Europol. Pridobljeno na https://www.europol.europa.eu/sites/default/files/publications/socta2013.pdf
8. Frideman, J. in Hoffman, D. V. (2008). Protecting data on mobile devices: A taxonomy of security threats to mobile computing and review of applicable defenses. *Information Knowledge Systems Management, 7*(1), 159–180.
9. F-Secure. (2013). *Mobile threat report*. Pridobljeno na http://www.f-secure.com/static/doc/labs_global/Research/Mobile_Threat_Report_Q3_2013.pdf
10. George, M. in Meadows, R. (2016). Policing on the surveillance frontier: Officer perspectives of body-worn cameras. *Revija za kriminalistiko in kriminologijo, 67*(4), 300–312.
11. GfK Group. (2011). *CEE Telco industry report 2011*. Pridobljeno na http://www.gfk.com/imperia/md/content/presse/pressemeldungen_2011/gfk_cee_telco_industry_report_en.pdf
12. Goswami, G., Vatsa, M. in Singh, R. (2017). Face verification via learned representation on feature-rich video frames. *IEEE Transactions on information forensics and security, 12*(7), 1686–1698.
13. Goodman, S. in Harris, A. (2010). Emerging markets: The coming African tsunami of information insecurity. *Communications of the ACM, 53*(12), 24–27.
14. Gradišar, M. in Lamberger, I. (2010). Vpliv represivnih dejavnikov na zlorabe kreditnih in plačilnih kartic v Sloveniji. *Revija za kriminalistiko in kriminologijo, 61*(1), 28–36.
15. Grizold, A. (1992). Oblikovanje slovenske nacionalne varnosti. V A. Grizold (ur.), *Razpotja nacionalne varnosti: obramboslovne raziskave v Sloveniji* (str. 59–93). Ljubljana: Fakulteta za družbene vede.
16. Hurlburt, G., Voas, J. in Miller, K. W. (2011). Mobile-app addiction: Threat to security? *IT Professional, 13*(6), 9–11.
17. International Data Corporation [IDC]. (2012). *Annual Report to Members.* Pridobljeno na http://www.idc.org/pdf/12_ici_annual.pdf
18. International Data Corporation [IDC]. (2014). *IDC – Press Release*. Pridobljeno na https://www.idc.com/getdoc.jsp?containerId=prUS24645514
19. International Data Corporation [IDC]. (2017). *IDC – Press Release*. Pridobljeno na https://www.idc.com/getdoc.jsp?containerId=prUS42628117
20. Japelj, B. (2016). Kriminaliteta v Sloveniji leta 2015. *Revija za kriminalistiko in kriminologijo, 67*(2), 140–170.
21. Juniper Networks. (2013). *Juniper Networks third annual mobile threats report: March 2012 through March 2013*. Pridobljeno na http://www.juniper.net/us/en/local/pdf/additional-resources/jnpr-2012-mobile-threats-report.pdf
22. Kazenski zakonik (KZ-1). (2012, 2015, 2016, 2017). *Uradni list RS,* (50/12, 54/15, 6/16, 27/17).
23. Kazenski zakonik (KZ-A). (1999). *Uradni list RS* (23/99).
24. Kazenski zakonik (KZ). (2004). *Uradni list RS,* (95/04).
25. Kolenc, T., Kebe, J. in Bukovnik, A. (2013). Kriminaliteta v Sloveniji v letu 2012. *Revija za kriminalistiko in kriminologijo, 64*(2), 95–121.
26. Konvencija Sveta Evrope o kibernetski kriminaliteti. (2004). *Uradni list RS,* (62/04-MP).
27. Lamberger, I., Slak, B. in Dobovšek, B. (2013). Kriminalistično preiskovanje spletnih goljufij s predplačili. *Revija za kriminalistiko in kriminologijo, 64*(2), 195–203.

28. Loo, A. (2009). Security threats of smart phones and bluetooth. *Communications of the ACM, 52*(3), 150–152.
29. Lukan, A. (2009). Kriminaliteta v letu 2008. *Revija za kriminalistiko in kriminologijo*, *60*(2), 77–90.
30. Markelj, B. (2014). *Grožnje informacijski varnosti pri rabi mobilnih naprav* (Doktorska disertacija). Ljubljana: Fakulteta za varnostne vede Univerze v Mariboru.
31. Markelj, B. in Bernik, I. (2011). Kombinirane grožnje informacijski varnosti pri rabi mobilnih naprav. V *Nove razmere in priložnosti v informatiki kot posledica družbenih sprememb: Zbornik 18. konference Dnevi slovenske informatike* (7 str.). Ljubljana: Slovensko društvo Informatika.
32. Markelj, B. in Završnik, A. (2016). Kibernetska korporativna varnost mobilnih naprav: Zavedanje uporabnikov v Sloveniji. *Revija za kriminalistiko in kriminologijo, 67*(1), 44–60.
33. McAfee. (2011). The rise of the virtual office. *Technology review.* Pridobljeno na http://www.technologyreview.com/news/424871/the-rise-of-the-virtual-office/
34. McAfee. (2012). *McAfee threats report: first quarter 2012*. Pridobljeno na http://www.McAfee.com/us/resources/reports/rp-quarterly-threat-q1-2012.pdf
35. McAfee. (2013). *Threats predictions*. Pridobljeno na http://www.f-secure.com/static/doc/labs_global/Research/Mobile_Threat_Report_Q3_2013.pdf
36. McAfee. (2014a). *McAfee Labs 2014 threats predictions.* Pridobljeno na http://www.mcafee.com/uk/resources/reports/rp-threats-predictions-2014.pdf
37. McAfee. (2014b). *McAfee Labs threats report*. Pridobljeno na https://www.mcafee.com/us/resources/reports/rp-quarterly-threat-q1-2014.pdf
38. McAfee. (2015a). McAfee Labs 2015 threats predictions. Pridobljeno na http://www.mcafee.com/ca/resources/misc/infographic-threats-predictions-2015.pdf
39. McAfee. (2015b). *McAfee Labs threats report*. Pridobljeno na https://www.mcafee.com/us/resources/reports/rp-quarterly-threat-q1-2015.pdf
40. McAfee. (2016). *McAfee Labs threats report*. Pridobljeno na https://www.mcafee.com/hk/resources/reports/rp-quarterly-threats-dec-2016.pdf
41. McAfee. (2017). *McAfee Labs threats report*. Pridobljeno na https://www.mcafee.com/us/resources/reports/rp-quarterly-threats-mar-2017.pdf
42. Meško, G. (2002). *Osnove preprečevanja kriminalitete*. Ljubljana: Visoka policijsko-varnostna šola.
43. Meško, G. in Bernik, I. (2011). Cybercrime: Awareness and fear: Slovenian perspectives. V N. Memon in D. Zeng (ur,). *2011 European intelligence and security informatics conference* (str. 28–33). Atene: IEEE Computer Society Press.
44. Policija. (2007). *Poročilo o delu Policije za leto 2006.* Pridobljeno na http://www.policija.si/images/stories/Statistika/LetnaPorocila/PDF/lp2006.pdf
45. Policija. (2008). *Poročilo o delu Policije za leto 2007.* Pridobljeno na http://www.policija.si/images/stories/Statistika/LetnaPorocila/PDF/LetnoPorocilo2007.pdf
46. Policija. (2009). *Poročilo o delu Policije za leto 2008.* Pridobljeno na http://www.policija.si/images/stories/Statistika/LetnaPorocila/PDF/LetnoPorocilo2008.pdf
47. Policija. (2010). *Poročilo o delu Policije za leto 2009.* Pridobljeno na http://www.policija.si/images/stories/Statistika/LetnaPorocila/PDF/LetnoPorocilo2009.pdf
48. Policija. (2011). *Poročilo o delu Policije za leto 2010.* Pridobljeno na http://www.policija.si/images/stories/Statistika/LetnaPorocila/PDF/LetnoPorocilo2010.pdf
49. Policija. (2012). *Poročilo o delu Policije za leto 2011.* Pridobljeno na http://www.policija.si/images/stories/Statistika/LetnaPorocila/PDF/LetnoPorocilo2011.pdf
50. Policija. (2013). *Poročilo o delu Policije za leto 2012.* Pridobljeno na http://www.policija.si/images/stories/Statistika/LetnaPorocila/PDF/LetnoPorocilo2012.pdf
51. Policija. (2014). *Poročilo o delu Policije za leto 2013.* Pridobljeno na http://www.policija.si/images/stories/Statistika/LetnaPorocila/PDF/LetnoPorocilo2013.pdf
52. Policija. (2015). *Poročilo o delu Policije za leto 2014.* Pridobljeno na http://www.policija.si/images/stories/Statistika/LetnaPorocila/PDF/LetnoPorocilo2014.pdf
53. Policija. (2016). *Poročilo o delu Policije za prvo polletje leta 2015.* Pridobljeno na http://www.policija.si/images/stories/Statistika/LetnaPorocila/PDF/PorociloZaPrvoPolletje2015.pdf
54. Resolucija o strategiji nacionalne varnosti Republike Slovenije (ReSNV-1). (2010). *Uradni list RS*, (27/10).
55. Riedy, M. K., Beros, S. in Wen H. J. (2011). Management business smarthphone data. *Journal of Internet Law*, *14*(9), 3–14.
56. Ritchey, D. (1. 3. 2012). Mobility madness: security and the smartphone. *SecurityMagazine.* Pridobljeno na http://www.securitymagazine.com/articles/82809-mobility-madness-security-and-the-smartphone
57. Schjolberg, S. (2010). *A Cyberspace Treaty: A United Nations Convention or Protocol on Cybersecurity and Cybercrime*. Pridobljeno na http://www.cybercrimelaw.net/documents/UN_12th_Crime_Congress.pdf
58. Smolič, M. in Mlinar, T. (2001). Storitve v mobilnih sistemih tretje generacije. *Življenje in tehnika*, *52*(4), 58–63.
59. Sotlar, A. (2008). Od globalne varnosti do individualne (ne)varnosti. *Delo in varnost, 53*(6), 8–16.
60. Sotlar, A. in Tominc, B. (2012). Zaznava deklarativnih virov ogrožanja nacionalne varnosti v slovenski družbi. *Varstvoslovje, 14*(3), 231–258.
61. Statistični urad Republike Slovenije. (2015). *Obsojene polnoletne osebe.* Pridobljeno na http://pxweb.stat.si/pxweb/Database/Dem_soc/13_kriminaliteta/90_arhiv/03_13603_obsojene_poln_osebe/03_13603_obsojene_poln_osebe.asp
62. Svet Evrope (2004). *Konvencija o kibernetski kriminaliteti.* Pridobljeno na http://conventions.coe.int/Treaty/en/Treaties/Html/185.htm.
63. Šugman, K. (2007). Pomen dokaznih standardov v kazenskem postopku. *Zbornik znanstvenih razprav Pravne fakultete v Ljubljani, 67*, 245–266.
64. Tang, Q. in Xu, X. (2012). Wireless multimedia communication requirements for police and PDT+LTE+3G solution. V W. Zhang, X. Yang, Z. Xu, P. An, Q. Liu in Y. Lu (ur.), *Advances on digital television and wireless multimedia communications* (str. 341–346). Berlin: Springer
65. Tiongson, J. (2015). Mobile app marketing insights: How consumers really find and use your apps. *Think with Google*. Pridobljeno na https://www.thinkwithgoogle.com/consumer-insights/mobile-app-marketing-insights/
66. Ustava Republike Slovenije. (1991, 1997, 2000, 2003, 2004, 2006 2013, 2016). Uradni list RS, (33/91, 42/97, 66/00, 24/03, 69/04, 69/04, 68/06, 47/13, 75/16).
67. Van Duyne, P. C. (2009). Old and new criminally mobile Europe. V P. C. van Duyne, S. Donati, J. Harvey, A. Maljevic in K. von Lampe (ur.), *Crime, money and criminal mobility in Europe* (str. 19–42). Nijmegen: Wolf Legal Publishers.

68. Vander Beken, T. in Daele, S. (2009). Out of step? Mobility of itinerant crime groups. V P. C. van Duyne, S. Donati, J. Harvey, A. Maljevic in K. von Lampe (ur.), *Crime, money and criminal mobility in Europe* (str. 43–70). Nijmegen: Wolf Legal Publishers.
69. Vidic, M. (2009). Uporaba interneta v teroristične namene. *Revija za kriminalistiko in kriminologijo, 60*(3), 211–222.
70. Vorderer, P., Kröemer, N. in Scheider, F. M. (2016). Permanently online – Permanently connected: Explorations into university students' use of social media and mobile smart devices. *Computers in Human Behavior, 63,* 694–703.
71. Wall, D. S. (2008a). Cybercrime and the culture of fear. *Information, Communication & Society, 11*(6), 861–884.
72. Wall, D. S. (2008b). Cybercrime, media and insecurity: The shaping of public perceptions of cybercrime. *International Review of Law, Computers and Technology, 22*(1–2), 45–63.
73. Weber, A. in Darbellay, A. (2010). Legal issues in mobile banking. *Journal of Banking Regulation, 11*(2), 129–145.
74. Završnik, A. (2005). Kibernetična kriminaliteta – (kiber) kriminološke in (kiber)viktimološke posebnosti »informacijske avtoceste«. *Revija za kriminalistiko in kriminologijo*, *53*(3), 248–260.

Cyber Security and Cyber Criminality of Mobile Device Users in Slovenia

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

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

Information technology (including mobile devices) has enabled the development of new forms of crime (cybercrime). The increased use of mobile devices for personal, business, even criminal purposes, as well as increased usefulness of mobile devices also have an impact on criminal law. It has to regulate appropriate definitions of criminal acts and general definitions, which cover the mobile device as the object of an attack and/or the means to commit a criminal act. The first part of the paper presents the results of a survey performed in the business sector among 34 Slovenian organisations on the use of mobile devices, and risks and use of appropriate methods of protection. The data show the state of the art threats to mobile devices in Slovenia and consequently the risk for cybercrime. The second part of the paper deals with this topic from the point of view of the criminal law. It discusses the regulation of the relevant criminal acts in the Criminal Code - 1 (2012) and presents the official statistical data from the Police and the Statistical Office of Slovenia regarding the processing of cybercrime. The conclusion offers solutions for the improvement of cyber security of mobile devices and decreasing the risk of cybercrime. The model of implementation of mobile devices into an organization, taking into consideration both the elements of information security and the variety and needs of work processes in such organizations.

Keywords: mobile devices, cyber security, cybercrime, criminal law

UDC: 343.3/.7:004