Slovenija in informacijska zasebnost ter kibernetska kriminaliteta v ožjem smislu v letih 2000 -2010

Zoran Cunk, Sektor kriminalistične policije Policijske uprave Maribor

Namen prispevka:
Prikazati želim zgodovinski primerjalno pravni pregled varstva informacijske zasebnosti in posledično pojavnosti kaznivih dejanj kibernetske kriminalitete v ožjem smislu iz KZ in KZ-1, katerih objekt kazenskopravnega varstva so informacijski sistemi in njihovi podatki. Tako želim prikazati bistveni kazalnik problematike napadov na informacijske sisteme in podatke kot varovane objekte informacijske zasebnosti ter kazenskopravni postopek v Sloveniji v obdobju od leta 2000 do leta 2010 in ponuditi dodatno orodje za celovitejšo obravnavo področja pravic (informacijske) zasebnosti.

Metodologija:
Za oblikovanje bistvenih spoznanj o integriteti informacijskega sistema in podatkov ter informacijske zasebnosti sem z opisno metodo uporabil strokovno literaturo in vire, ki se nanašajo na tematiko prispevka. Za proučitev stanja kibernetske kriminalitete v ožjem smislu na območju Slovenije v obravnavanem obdobju pa so bili z analitično metodo ustrezno obdelani sekundarni podatki.

Ugotovitve in omejitve:
Pri obravnavi kaznivih dejanj kibernetske kriminalitete v ožjem smislu se bomo osredotočili na obravnavo kaznivih dejanj polnoletnih osumljencev/obtožencev/obsojencev s strani bistvenih deležnikov kazenskega postopka v Sloveniji: državnih tožilstev ter sodišč, pozornost pa bomo namenili tudi prikazu izrečenih pravnomočnih kazenskih sankcij. Glede na predstavljene podatke je bistvena ugotovitev, da je kazenskih postopkov kaznivih dejanj kibernetske kriminalitete v ožjem smislu relativno malo, kar je posledica tudi/predvsem neozaveščenosti ljudi in sram pred vlogo oškodovanca kaznivega dejanja.

Izvirnost/pomembnost prispevka:
Prispevek spremlja kazniva dejanja kibernetske kriminalitete v ožjem smislu na območju Slovenije v relativno dolgem časovnem obdobju 10. let, ki že omogoča ustvarjanje jasne slike o obravnavi kazenskopravne pojavnosti ter odpira vprašanje odkrivanja in preiskovanja neraziskanih in neodkritih kaznivih dejanj.

Ključne besede: informacijska tehnologija in zasebnost, kaznivo dejanje

1 UVOD

Informacijska tehnologija, kot kompleksna celota postopkov in naprav za oskrbovanje uporabnika s potrebnimi podatki, je temeljna značilnost in bistven proizvod informacijske dobe, v kateri se nahajamo. Naprave oziroma informacijsko tehnologijo predstavljajo med drugim radio, televizija, telefon, splet, elektronska pošta in drugo, vendar je potrebno poudariti, da je danes računalnik bistven predstavnik informacijske tehnologije. Računalnik se tako vsakodnevno uporablja v vlogi:

- naprave za avtomatsko obdelavo, shranjevanje in prenos raznovrstnih podatkov v digitalni obliki;
- vedno pomembnejšega sredstva (individualnega in množičnega) komuniciranja, kot najuspešnejšega in najučinkovitejšega komunikacijskega kanala za doseganje cilja, hitrega in celovitega (pisnega, zvočnega, slikovnega), prenosa podatkov, informacij in znanja na daljavo.

Ravno razvoj računalnika s širjenjem področij njegove uporabe (ne samo v osebnem življenju posameznika, temveč in predvsem tudi na njegovem poslovnem, državnem in mednarodnem področju), pa vedno bolj intenzivno in kompleksno posega tudi na področje zasebnosti uporabnika računalnika. Kovačič (2006, 12) sicer ugotavlja, da univerzalne definicije zasebnosti in pravice do zasebnosti ni, saj je zasebnost relativna, kontekstualna in subjektivna, zaradi česar se pravna teorija

izogiba natančnemu definiranju pravice do zasebnosti, celo več, natančno definiranje zasebnosti niti ni zaželeno. Ob tem Završnik (2010, 6) poudarja, da je za sodobno pojmovanje zasebnosti ključno, da je prežeta s posesivnim individualizmom, zasebno lastnino in dvomljivim pojmovanjem osebe, kot avtonomne, od družbe ločene entitete, Klemenčič (2003, 101) pa opozarja, da vprašanje zasebnosti v t.i. informacijski družbi predstavlja enega od ključnih pravnih, sociooloških, filozofskih in etičnih vprašanj sodobne družbe, vendar je jasno, da ko govorimo o zasebnosti, mislimo predvsem na pravico do zasebnosti.

Lampe (2003, 121-122) tako opredeli pravico do zasebnosti kot elementarno človekovo pravico – tako mednarodno kot ustavno pravico javnopravnega značaja ter osebnostno pravico civilnopravnega značaja, kot eno izmed nepogrešljivih elementov človekove eksistence, ki varuje človeka pred prekomernimi posegi državne oblasti, javnosti in drugih posameznikov v posameznikovo odločitveno, duševno, prostorsko in informacijsko zasebnost. Informacijsko zasebnost razdeli v dve temeljni skupini (Lampe, 125-130):

- prvo, kamor uvrščamo dve obliki informacijske zasebnosti in sicer:
    - korespodenčno, kjer posameznik v osebnih pisanjih ali izjavah kot tudi v korespodenci (tudi s časovnih zamikom) izraža marsikaj iz svoje duševne zasebnosti, svoje intime, ki jo ne namenja tretjim posameznikom ali širši javnosti, temveč le določeni osebi, kateri piše; in
    - komunikacijsko, kjer izmenjava informacij poteka med najmanj dvema posameznikoma brez časovnega zamika ter običajno ustno, kot pogovor z uporabo glasu ali tudi pisno preko ustreznih tehničnih sredstev (npr. chat rooms);
- drugo, kamor uvrščamo zasebnost varstva podatkov (data privacy), torej tistih podatkov, ki se hranijo v posebnih zbirkah, ki so avtomatično ali sistematično obdelani

Kako je torej varnost informacijske zasebnosti urejena v Sloveniji?

2 UGOTOVITVE

V Sloveniji je zasebnost (tako kot v večini evropskih držav) ustavna kategorija (Kovačič 2006, 71). Ustava Republike Slovenije (Ur. l. RS 331/1991), informacijsko zasebnost varuje z določili:

- 37. člena Ustave (varnost tajnosti pisem in drugih občil), ki zagotavlja pravico do komunikacijske zasebnosti in ki v prvi vrsti predstavlja varstvo posameznikovega interesa, da se država ali nepovabljeni tretji ne seznanijo z vsebino sporočila, ki ga posreduje preko kateregakoli sredstva, ki omogoča izmenjavo oziroma posredovanje informacij, kot tudi posameznikovega interesa, da ima nadzor nad tem, komu, v kakšnem obsegu, na kakšen način in pod kakšnimi pogoji bo posredoval določeno sporočilo (Klemenčič 2010, 391); in
- 38. člena Ustave (varnost osebnih podatkov), ki v obravnavanem členu zagotavlja varstvo osebnih podatkov in ki se odraža v zahtevi po zakonitosti zbiranja, obdelave in uporabe osebnih podatkov in v zahtevi po njihovem zbiranju in uporabi za vnaprej določene namene, posamezniku pa daje tudi pravico do seznanjenosti o tem, kateri podatki se zbirajo o njem, in pravico do sodnega varstva (Čebulj 2010, 409).

Vrste in obseg pravic, ki jih ima posameznik, da bi lahko uresničeval varstvo informacijske zasebnosti, so določene z zakonom. Pravica do zasebnosti ima tako absolutni značaj, kar pomeni, da deluje proti vsem – *erga omnes*, tako proti državnim organom (vertikalno razmerje) kot tudi nasproti tretjim osebam (horizontalno razmerje) (Lampe 2003, 12). Država lahko ob izpolnitvi določenih predpostavk (v skladu z načelom sorazmernosti, če je omejitev potrebna in nujna za dosega zasledovanega ustavno legitimnega cilja (Čebulj 2010, 411) posega v zasebno sfero posameznika, v praksi pa se zgodi, da to protipravno izvede tudi posameznik. Informacijska tehnologija je človeštvu sicer prinesla veliko koristi, hkrati pa so vzniknile tudi nove oblike kriminalitete (Završnik 2007, 457-463). Država zato kot bistven objekt zaščite, informacijsko zasebnost varuje tudi kazenskopravno. Svetovna mrežna povezanosti informacijskih sistemov je tudi razlog, da so prizadevanja za ustrezno kazenskopravno varnost prestopila nacionalne meje in le-te pričela urejati tudi na mednarodni ravni s Konvencijo o kibernetski kriminaliteti (Ur. l. RS, MP 17/2004). Poglejmo, kako so se pravila in zahteve po varstvu informacijske zasebnosti izrazile v kazenskem materialnem pravu (teoretično in praktično).

Uveljavljena filozofska disciplina – etika, in v okviru nje izoblikovana informacijska etika, ne ustrezata sliki dejanske uporabe v vsakdanjem življenju, zato številne civilnopravne norme s svojo zgodovinsko utemeljeno funkcijo varstva uporabnika informacijske tehnologije kot posebej zaščitenega udeleženca ustvarjanja, uporabe in hranjenja podatkov in informacij, določajo minimum pravic informacijske zasebnosti. Kibernetska kazniva dejanja sicer obsegajo večje število kaznivih dejanj, tudi v odvisnosti od opredelitve termina kibernetske kriminalitete, v našem prispevku pa se bomo osredotočili na t.i. kibernetsko kriminaliteto v ožjem smislu. Ta vključuje kriminaliteto, ki ogroža informacijsko in omrežno varnost, objekt kazenskopravnega varstva pa so informacijski sistemi in računalniški podatki (Završnik 2007, 461-489). KZ (Ur. l. RS, št. 63/94 s spremembami) in KZ-1 (Ur. l. RS, štev. 55/2008 s spremembami) tako med drugimi obravnavata tudi kršitve informacijskih pravic uporabnikov informacijske tehnologije na področju protipravnega dostopa, protipravnega prestrezanja, motenja podatkov, motenja sistemov ter zlorabe naprav kot pripravljalnih dejanj, povezanih s temi ravnanji, ki izpolnjujejo znake kaznivega dejanja.

Kaznivo dejanje kot najtežje kaznivo ravnanje je KZ opredeljeval kot protipravno dejanje, ki ga zakon zaradi njegove nevarnosti določa kot kaznivo dejanje in hkrati določa njegove znake in kazen zanj (7. člen KZ), medtem ko ga KZ-1 opredeljuje kot človekovo protipravno dejanje, ki ga zakon zaradi nujnega varstva pravnih vrednot določa kot kaznivo dejanje in hkrati določa njegove znake ter kazen za krivega storilca (16. člen KZ-1). Uporabnik informacijskega sistema se v vlogi oškodovanca, torej osebe, kateremu je kakršnakoli njegova osebna ali premoženjska pravica s kaznivim dejanjem prekršena ali ogrožena (144. člen Zakona o kazenskem postopku, Ur. l. RS, št. 63/1004 s spremembami), zaradi kršenja njegovih informacijskih pravic (pravice do integritete informacijskega sistema in podatkov ter s tem pravice do informacijske zasebnosti), lahko pojavi v naslednjih ravnanjih, ki imajo znake kaznivega dejanja (prirejeno po Cunk 2010, II):

1. Neupravičen vstop v zaščiteno računalniško bazo podatkov po členu 225 KZ in Napad na informacijski sistem po členu 221 KZ-1 (kot izhodiščno kaznivo dejanje zoper zaupnost, celovitost in dostopnost računalniških podatkov in sistemov z različnimi oblikami protipravnega dostopa, protipravnega prestrezanja, motenja podatkov in motenja sistemov – v nadaljevanju napad na informacijski sistem).
2. Vdor v računalniški sistem po členu 242 KZ in v vdor v poslovni informacijski sistem po členu 237 KZ-1 (kot specialna oblika prejšnjega kaznivega dejanja, t.i. industrijsko vohunstvo - v nadaljevanju industrijsko vohunstvo).
3. Zloraba osebnih podatkov po drugem in tretjem odstavku 154 člena KZ ter po drugem in petem odstavku 143 člena KZ-1 (obarvan naklep pri storitvi sicer drugega temeljnega kaznivega dejanja, kjer pa je namen vdora pridobitev osebnih podatkov – v nadaljevanju vdor za osebne podatke).
4. Izdelovanje in pridobivanje orožja in pripomočkov, namenjenih za kaznivo dejanje po členu 309 KZ oziroma členu 306 KZ-1 (kot pripravljalno dejanje vendar opredeljeno kot samostojno kaznivo dejanje – v nadaljevanju posest pripomočkov).

Čeprav so splošni objekti kazenskopravnega varstva navedenih kaznivih dejanj v KZ in KZ-1 različni, si v nadaljevanju poglejmo bistvene skupne značilnosti teh kaznivih dejanj:

- za storilca kaznivega dejanja je uporabljena najsplošnejša označba »kdor«. Kaznivi dejanji napada na informacijski sistem nesporno sodita med splošna kazniva dejanja (***delicta communia***), za katera je značilno, da jih lahko stori vsaka oseba, ki je lahko subjekt kazenskega prava. Za storilca kaznivega dejanja industrijskega vohunstva pa je sicer takšna označba presplošna, saj je opis posameznega kaznivega dejanja z dodajanjem posebnih osebnih ali pravnih lastnosti storilca sestavljen tako, da vsebinsko pomeni določitev ***delicta propria***. Dejstvo, da mora biti dejanje storjeno pri gospodarskem poslovanju, namreč zoži krog možnih storilcev na osebe, ki se ukvarjajo s tovrstno dejavnostjo ali sodelujejo pri taki dejavnosti (VSL0023138). Pomembna je tudi sodba Vrhovnega sodišča (VS23600), ki poudarja, da kaznivo dejanje vdora v računalniški sistem lahko stori kdorkoli in ne samo oseba, ki od zunaj vdre v računalnik, torej tudi oseba, ki program upravlja v okviru svojih delovnih dolžnosti. Lampe (2003, 170) to potrjuje, ko navaja, da je pri vdorih v računalniške sisteme zanimivo to, da 70-80% vdorov povzročijo zaposleni;

- neupravičen vstop oziroma vdor lahko storilec izvrši neposredno iz prostora (zgradbe), kjer je informacijski sistem nameščen, lahko pa to izvrši prek medmrežja oziroma interneta. Poseg je tako lahko naperjen na podatke, na delovanje programov in na delovanje samega sistema;
- storilec lahko kazniva dejanja stori le naklepno, saj dikcije predpostavljajo zavest o protipravnosti ravnanja;
- kazniva dejanja so poškodbena kazniva dejanja, ki se praviloma kažejo v nastali (premoženjski) škodi za oškodovanca; in
- za kazniva dejanja napada na informacijski sistem in industrijske špijunaže, v skladu z Zakonom o odgovornosti pravnih oseb za kazniva dejanja (Ur. l. RS, št. 59/1999 s spremembami) lahko odgovarjajo tudi pravne osebe.

Poudariti je potrebno, da se prav vsa, zgoraj navedena kazniva dejanja s področja varstva informacijskega sistema in podatkov, preganjajo po uradni dolžnosti.

V nadaljevanju se bomo osredotočili na pojavnost kaznivih dejanja kibernetske kriminalitete v ožjem smislu v Sloveniji s prikazom odločb državnih tožilstev pri obravnavi ovadenih polnoletnih oseb in odločb sodišč pri obravnavi polnoletnih obtoženih oseb z izrečenimi kazenskimi sankcijami obsojenim polnoletnim osebam v obdobju od leta 2000 do leta 2010 (Statistični urad Republike Slovenije (SURS), lastni izračun).

Državna tožilstva so tako v navedenem obdobju končala postopke za kazniva dejanja:

- napada na informacijski sistem za 342 osumljencev. Za kar 197 osumljencev (57,6 odstotka) so končala postopek za neznanega storilca, za 96 osumljencev (28,07 odstotka) so postopek končala z zavrženjem ovadbe, za šest osumljencev (1,75 odstotka) so postopek končala z odstopom tuji državi, za enega osumljenca (0,29 odstotka) so postopek rešila na drug način, za 42 osumljencev (12,28 odstotka) pa so vložila obtožni akt.
- industrijskega vohunstva za 67 osumljencev. Za 33 osumljencev (49,25 odstotka) so končala postopek za neznanega storilca, za 27 osumljencev (40,3 odstotka) so postopek končala z zavrženjem ovadbe, za enega osumljenca (1,49%) so preiskavo ustavila, za šest osumljencev (8,96 odstotka) pa so vložila obtožni akt.
- vdora za osebne podatke za 52 osumljencev. Za 38 osumljencev (73,08 odstotka) so postopek končala z zavrženjem ovadbe, za štiri osumljence (7,69 odstotka) so končala postopek za neznanega storilca, za 10 osumljencev (19,23 odstotka) pa so vložila obtožni akt.
- posesti pripomočkov za 17 osumljencev. Za tri osumljence (17,8 odstotka) so postopek končala za neznano osebo, za enega osumljenca (5,88 odstotka) so postopek končala z zavrženjem ovadbe, za 13 osumljencev (76,47 odstotka) pa so vložila obtožni akt.

Sodišča so v navedenem obdobju končala postopke za kazniva dejanja:

- napada na informacijski sistem za 34 obtožencev. Sodišča so za pet obtožencev (14,71 odstotka) postopek ustavila, za štiri obtožence (11,76 odstotka) so obtožbo zavrnila, za po tri obtožence (8,82 odstotka) so obtožbo zavrgla oziroma obtožence oprostila, 18 obtožencev (52,94 odstotka) pa so spoznala za krive.
- Industrijskega vohunstva za šest obtožencev. Sodišča so postopek ustavila za dva obtoženca (33,33 odstotka), enega obtoženca so sodišča oprostila (16,67 odstotka), tri obtožence (50 odstotkov) pa so spoznala za krive.
- vdora za osebne podatke za tri obtožence. Za 2 obtoženca (66,67 odstotka) so postopek ustavila, enega obtoženca pa so sodišča oprostila (33,33 odstotka).
- posesti pripomočkov za 16 obtožencev. Sodišča so za dva obtoženca (12,5 odstotka) postopek ustavila, obtožbo so sodišča za enega obtoženca (6,25 odstotka) zavrnila, 13 obtožencev (81,25 odstotka) pa so spoznala za krive

Sodišča so izrekla naslednje kazenske sankcije obsojencem za kazniva dejanja:

- napada na informacijski sistem: 13. obsojencem (72,22 odstotka) opozorilno sankcijo - pogojno zaporno sodbo (dvema nad 6 mesecev do 1 leta, sedmim nad 3 mesece do 6 mesecev, dvema nad 1 meseca do 2 meseca in dvema do 30 dni), po enemu obsojencu (5,56 odstotka) pa denarno kazen (leta 2003), zaporno kazen (nad 6 mesecev do 1 leta), sodni opomin in drugo kazensko sankcijo. Leta 2005 so obsojencu izrekla kot stransko kazen denarno kazen.
- Industrijskega vohunstva: vsem trem obsojencem opozorilno sankcijo - pogojno zaporno sodbo nad 3 mesece do 6 mesecev.

- posesti pripomočkov: osmim obsojencem (61,54 odstotka) opozorilno sankcijo - pogojno zaporno sodbo (trem nad 3 mesece do 6 mesecev, štirim nad 1 mesec do 2 meseca in enemu do 30 dni), štirim obsojencem (30,77 odstotka) zaporno kazen (enemu nad dve leti do treh let in trem nad 1 leto do dveh let) in enemu obsojencu (7,69 odstotka) sodni opomin. Enemu obsojencu (leta 2008) je bil kot stranska kazen izrečen ukrep izgona tujca iz države, varnostni ukrep odvzema predmetov pa je bil izrečen petim obsojencem.

3 SKLEP

Zgodovinski primerjalno pravni pregled gibanja kaznivih dejanj iz KZ in KZ-1, zoper integriteto informacijskih sistemov in podatkov v obdobju 2000-2010, nam torej kaže (SURS, lastni izračun):

1. kaznivi dejanji napada na informacijski sistem: tožilstva so letno končala postopek za povprečno 31 osumljencev, za povprečno štiri osumljene letno pa so vložila obtožni akt. Sodišča so letno spoznala za kriva povprečno dva obtoženca. V obdobju 2000-2010 je bilo od celotnega števila osumljencev 5,26 odstotka spoznanih za krive.
2. kaznivi dejanji industrijskega vohunstva: tožilstva so letno končala postopek za povprečno šest osumljencev. V celotnem obdobju so za skupaj šest osumljencev tožilstva vložila obtožni akt. Sodišča so spoznala za krive skupaj tri obtožence. V obdobju 2000-2010 je bilo od celotnega števila osumljencev 4,48 odstotka obsojenih.
3. kaznivi dejanji vdora za osebne podatke: tožilstva so v obravnavanem obdobju končala postopek za skupaj 51 osumljencev. Za 10 osumljencev so tožilstva vložila obtožni akt. Sodišča so v celotnem obdobju končala postopek za 3 obtožence, nobenega pa niso spoznala za krivega;
4. kaznivi dejanji posesti pripomočkov: tožilstva so v obdobju končala postopek za 17 osumljencev. Za povprečno enega osumljenca letno so tožilstva vložila obtožni akt. Sodišča so spoznala za krive skupaj 13 obtožencev. V obdobju 2000-2010 je bilo od celotnega števila osumljencev po tretjem odstavku člena 76,47 odstotka obsojenih.

Pomembni pa sta še značilnosti:

- veliko število kaznivih dejanj zaključenih za neznanega storilca (pri kaznivih dejanjih napada na informacijski sistem je tako zaključenih postopkov kar 57,6 odstotka in pri kaznivih dejanjih industrijskega vohunstva 49,24 odstotka osumljencev);
- ker je kaznivo dejanje kibernetske kriminalitete v ožjem smislu mogoče izvršiti zgolj z informacijsko tehnologijo ni izrečenega varnostnega ukrepa odvzema predmetov (razen pri kaznivih dejanjih posesti pripomočkov).

Nedvomno je ob teh podatkih o gibanju kaznivih dejanj kibernetske kriminalitete v ožjem smislu nujno potrebno upoštevati veliko območje neraziskanih in neodkritih kaznivih dejanj. K temu lahko veliko pripomore ozaveščanje ljudi. Izobraževanje in usposabljanje o nevarnosti kibernetske kriminalitete mora na vseh ravnem družbenega življenja postati del vsakdana (Bernik in Meško 1011, 250). S tem bomo namreč naredili bistven korak naprej pri obravnavi »kibernetskega prostora v miselnih tokovih postmodernistične teorije storilca, vključno s hekersko vredno(s)tno (o)pozicijo (Završnik 2009, 113)«. Odkrita pojavnost kaznivih dejanj pa ni (ne bi smela biti) izključno in samo v domeni zaznave oškodovanca in njegove izkazane volje po kazenskem pregonu, temveč mora država v okviru svojih institucij aktivno poskrbeti, da je vsaj spoštovanje minimalnih pravic informacijske zasebnosti, ki jih je tudi kazenskopravno zavarovala, nujno udejanjeno.

VIRI

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.

Cunk, Z. (2011). Kazenskopravni vidik varstva integritete informacijskega sistema in podatkov v Sloveniji: obdobje 2000-2009. Pravna praksa, 8(3.3.2011), II-VIII.

Čebulj, J. (2010). 38. člen (varstvo osebnih podatkov), V L. Šturm, L. (ur.), Komentar Ustave Republike Slovenije (str. 408-416), Kranj: Fakulteta za državne in evropske študije.

Klemenčič, G. (2003). Internet in pravica do zasebnosti, V B. Makarovič (ur.), Internet in pravo (str. 101-118), Ljubljana: Pravna fakulteta.
Klemenčič, G. (2010). 37. člen (varstvo tajnosti pisem in drugih občil), V L. Šturm (ur.), Komentar Ustave Republike Slovenije (str. 391-408), Kranj: Fakulteta za državne in evropske študije.
Konvencija o kibernetski kriminaliteti, Ur. l. RS, MP 17/2004. Pridobljeno 18.11.2010 na www.soe.si/sl/dokumenti_in_publikacije/konvencije/185.
Kazenski zakonik (KZ), Ur. l. RS, št. 63/94 s spremembami.
Kazenski zakonik (KZ-1), Ur. l. RS, štev. 55/2008 s spremembami.
Kovačič, M. (2006). Nadzor in zasebnost v informacijski družbi: informacijski, sociološki, pravni in tehnični vidiki nadzora in zasebnosti na internetu. Ljubljana: Fakulteta za družbene vede.
Lampe, R. (2003). Pravni in drugi izzivi informacijske družbe, V D. Lesjak (ur.), Pravna informatika: zapiski predavanj (str. 120-151), Maribor: Pravna fakulteta.
Statistični urad Republike Slovenije. (2000-2010). Polnoletne osebe zoper katere je bil kazenski postopek pravnomočno končan: Letna poročila. Pridobljeno 18.11.2009 in 14.12.2011 na http://www.stat.si/tema_demografsko_kriminaliteta.asp.
Ustava Republike Slovenije, Ur. l. RS 331/1991.
VSL0023138 (VSL sodba III Kp 6/2008).
VS23600 (Sodba I Ips 396/2005).
Zakon o kazenskem postopku (ZKP), Ur. l. RS, št. 63/1004 s spremembami.
Zakon o odgovornosti pravnih oseb za kazniva dejanja, Ur. l. RS, št. 59/1999 s spremembami.
Završnik, A. (2007). Problemi kibernetske kriminalitete, V A. Šelih, Sodobne usmeritve kazenskega materialnega prava. Ljubljana: Inštitut za kriminologijo pri Pravni fakulteti.
Završnik, A. (2009). Homo criminalis: upodobitve zločinskega subjekta v visokotehnološki družbi tveganja. Ljubljana: Inštitut za kriminologijo pri Pravni fakulteti.
Završnik, A. (2010). Kriminaliteta in tehnologija: Uvod, V A. Završnik (ur.), Kriminaliteta in tehnologija: kako računalniki spreminjajo nadzor in zasebnost, ter kriminaliteto in kazenski pregon? (str. 1-21), Ljubljana: Inštitut za kriminologijo pri Pravni fakulteti