*Kriminalističke teme*
*Zbornik radova*
Godina XIX, Broj 5, 2019.
ISSN 1512-5505



# STANJE, KRETANJE I NORMATIVNO UREĐENJE RAČUNALNOG KRIMINALITETA U REPUBLICI HRVATSKOJ

STATE, TRENDS AND NORMATIVE REGULATION OF CYBERCRIME IN THE REPUBLIC OF CROATIA

**Izvorni naučni rad**

**dr. sc. Mirjana Kondor-Langer**[39]
**dr.sc. Krunoslav Borovec**[40]
**dr. sc. Stjepan Gluščić**[41]

**SAŽETAK**

**Inspiracija za rad i problem (i) koji se radom oslovljava (ju):** U radu se kroz tri cjeline analiziraju odredbe Kaznenog zakona Republike Hrvatske, podaci o broju prijavljenih i razriješenih kaznenih djela prema službenoj statistici te se analiziraju rezultati provedenog istraživanja o svjesnosti računalnog kriminaliteta.

**Ciljevi rada (naučni i/ili društveni):** Ciljevi istraživanja nastojali su utvrditi navike mladih vezane za korištenje interneta; ispitati njihovu svijest i iskustva o opasnostima računalnog (*cyber*) kriminaliteta; utvrditi razinu viktimizacije računalnim kriminalitetom te utvrditi postoji li veza između negativnih iskustava na internetu te eventualne viktimizacije s promjenom ponašanja prilikom korištenja interneta.

**Metodologija/Dizajn:** Istraživanje je provedeno na prigodnom uzorku od 344 ispitanika, studenata veleučilišta i visokih škola u Republici Hrvatskoj. Rezultati dobiveni ovim istraživanjem obrađeni su u statističkom programu SPSS, a u radu su prikazani rezultati deskriptivne statistike, marginalne frekvencije odgovora ispitanika na pojedina pitanja. Radi utvrđivanja postojanja veza između negativnih iskustava na internetu te eventualne viktimizacije s promjenom ponašanja prilikom korištenja interneta korišten je hi-kvadrat test, kao test nezavisnosti dviju varijabli.

**Ograničenja istraživanja/rada:** ograničenja ovog istraživanja ogledaju se u činjenici da je istraživanjem obuhvaćena specifična skupina mladih (studenti visokih učilišta), čija se ponašanja i iskustva povezana s internetom ne mogu generalizirati na širu populaciju, tako da i dobivene rezultate treba promatrati u kontekstu ovog ograničenja. S druge pak strane, podaci o broju prijavljenih i razriješenih kaznenih djela, prikupljeni iz službenih policijskih statistika, također imaju ograničenje jer se ne odnose na ukupni, već samo registrirani kriminalitet.

**Rezultati/Nalazi:** Provedeno istraživanje pokazalo je da je 46,8 % ispitanika neprekidno na internetu te da njih 54,9 % svoje informacije na internetu ne doživljava sigurnim, a 18,4 % ispitanika bilo je žrtvom računalnog kriminaliteta.

[39] Visoka policijska škola u Zagrebu, mklanger@fkz.hr
[40] Visoka policijska škola u Zagrebu, kborovec@mup.hr
[41] Visoka policijska škola u Zagrebu, sgluscic@fkz.hr

**Generalni zaključak:** Podaci pokazuju vrlo visok stupanj uspješnosti u razjašnjavanju prijavljenog kriminaliteta te visok stupanj svjesnosti o opasnostima novih tehnologija ali i relativno neadekvatnu zaštitu.
**Opravdanost istraživanja:** Računalni kriminalitet u Republici Hrvatskoj je za policiju važno područje. U tom području mogu se postići značajni pomaci upravo jačanjem prevencije i rada sa potencijalnim žrtvama kako bi se stvorilo povjerenje između policije i građana (tamo gdje ne postoji) te kako bi se otklonile zaprjeke za prijavljivanje kaznenih djela i suradnju tijekom istraživanja istih.

**KLJUČNE RIJEČI**
računalni kriminalitet, kaznena djela, stanje i kretanje kriminaliteta, informacijska sigurnost

**ABSTRACT**
**The inspiration for the paper and the problem (s) that the paper addresses:** The first part of the paper gives an analysis of the provisions of the Criminal Code of the Republic of Croatia. Furthermore the paper presents data on the reported and resolved computer crime according to official statistics and the results of the conducted research on computer crime awareness.
**The goals of the paper (scientific and/or social):** The research goals sought to determine youth habits related to Internet use; examine their awareness and experience of the dangers of cybercrime; determine the level of cybercrime victimization and determine if there is a link between negative experiences on the internet and any possible victimization with behavior change when using the internet.
**Methodology/Design:** The research sample included a convenience sample of 344 respondents, students of polytechnics and colleges in the Republic of Croatia. The results obtained by this research were analyzed in the SPSS statistical program. The paper presents the results of descriptive statistics and the marginal frequency of respondents' answers to a particular question. Two tests were used to determine whether there are links between negative experiences on the Internet and possible victimization with behavioural change when using the Internet- the chi-square test and the test of the independence of two variables.
**Research/the paper limitations:** The limitations of this research are reflected in fact that the respondents are only students from Croatian Colleges whose behaviours and experiences related to the use of Internet cannot be generalized to the general population. Therefore, the obtained results should be viewed in the context of these limitations. On the other hand, reported and discovered crimes data were collected from official police database and they do not present total but only registered crime.
**Results/findings:** The conducted research showed that 46.8% of the respondents were constantly on the Internet. 54.9% of them do not consider their information on the internet to be secure, and 18.4% of the respondents were victims of cybercrime.
**General conclusion:** The conducted research showed a high level of success in resolving reported crime and a high level of awareness of the dangers of new technologies, but it also drew attention to the inadequate level of cybersecurity.
**Research/the paper justifiability:** Computer crime in the Republic of Croatia is an important area for the police. Significant progress can be made in this area by strengthening prevention and by working with potential victims. That would create trust between police and citizens (where it does not exist), remove obstacles to reporting crimes and facilitate cooperation during the investigation of those types of crime.

**KEY WORDS**
cybercrime, computer crime, criminal offenses, crime trends, IT security

## 1. Uvodne napomene

U ovom radu, koji je suštinski podijeljen u tri cjeline analiziraju se odredbe Kaznenog zakona, podaci o broju prijavljenih i razriješenih kaznenih djela prema službenoj statistici Ministarstva unutarnjih poslova Republike Hrvatske i u trećem dijelu prikazuju se i analiziraju rezultati provedenog istraživanja o svjesnosti računalnog kriminaliteta. Istraživanjem su ispitane navike mladih vezane za korištenje interneta (svijest i iskustva o opasnostima računalnog (*cyber*) kriminaliteta, razina viktimizacije računalnim kriminalitetom te veza između negativnih iskustava na internetu te eventualne viktimizacije s promjenom ponašanja prilikom korištenja interneta), (o problematici pojmovnog određenja ovog područja, vidi više: Dragičević, D. (2004); Vuković, H. (2012).; Kokot, I. (2014)).

Kaznena djela iz područja računalnog kriminaliteta u Republici Hrvatskoj normirana su Kaznenim zakonom (Narodne Novine br. 125/11, 144/12, 56/15, 61/15, 101/17, 118/18; u daljnjem tekstu KZ RH) u Glavi XXV i usko su povezana uz računalnu tehnologiju i internet. Globalna i sveopća dostupnost računalne tehnologije dovodi do povećanja kaznenih djela kod kojih računalo služi kao sredstvo počinjenja kaznenog djela (vidi: Vuletić, I. (2014); Krapac, D. (1992)). Upravo stoga vrlo značajan međunarodni izvor za normiranje računalnog kriminaliteta predstavlja Konvencija o kibernetičkom kriminalu Vijeća Europe[42] i dodatni protokol uz Konvenciju o kibernetičkom kriminalu o inkriminiranju djela rasističke i ksenofobne naravi počinjenih pomoću računalnih sustava.[43]

Tako Vojković i Štambuk-Sunjić (2006:124) navode kako je jedan od ključnih događaja stupanje na snagu Konvencije o kibernetičkom kriminalu kojom se regulira potreba vođenja zajedničke kaznene politike u sferi borbe protiv računalnog kriminala. Republika Hrvatska je ratificirala Konvenciju o kibernetičkom kriminalu te njene odredbe unijela u svoj KZ RH donošenjem Zakona o izmjenama i dopunama Kaznenog zakona (Narodne novine, br. 105/04), a koji je stupio na snagu 1. listopada 2004. godine.

## 2. Normativno uređenje računalnog kriminaliteta u RH

Normativno uređenje računalnog kriminaliteta u Republici Hrvatskoj može se podijeliti na tri područja. Prva dva čine područja kaznenog i kaznenog procesnog prava (o problematici dokazivanja ovih kaznenih djela kao i korištenju dostignutih tehničkih mogućnosti napisani su brojni radovi; za primjer vidi: Čizmić, J., Boban, M. (2017)). Treće se područje odnosi na posebno zakonodavstvo koje pokriva sigurnosna i organizacijska pitanja kao i pitanje uređenja zaštite specifičnih prava. Tu je niz zakona i podzakonskih akata koja

[42] https://www.coe.int/en/web/conventions/full-list/-/conventions/rms/0900001680081561)
[43] (https://www.coe.int/en/web/conventions/full-list/-/conventions/rms/090000168008160f).

uređuju informacijsku sigurnost kao na primjer: Zakon o informacijskoj sigurnosti (Narodne Novine, br. 79/07), Zakon o provedbi Uredbe (EU) br. 910/2014 Europskog parlamenta i Vijeća od 23. srpnja 2014. o elektroničkoj identifikaciji i uslugama povjerenja za elektroničke transakcije na unutarnjem tržištu i stavljanju izvan snage Direktive 1999/93/EZ (Narodne Novine, br. 62/17), Zakon o elektroničkoj ispravi (Narodne Novine, br. 150/05), Zakon o elektroničkom novcu (Narodne Novine, br. 64/18), Zakon o tajnosti podataka (Narodne Novine, br. 79/07, 86/12), Zakon o provedbi Opće Uredbe o zaštiti podataka (Narodne Novine, br. 42/18), Zakon o pravu na pristup informacijama (Narodne Novine, br. 25/13, 85/15), Zakon o autorskom pravu i srodnim pravima (Narodne Novine, br. 167/03, 79/07, 80/11, 141/13, 127/14, 62/17, 96/18), Zakon o elektroničkoj trgovini (Narodne Novine, br. 173/03, 67/08, 36/09, 130/11, 30/14, 32/19) Zakon o elektroničkom izdavanju računa u javnoj nabavi (Narodne Novine, br. 94/18). O značaju ovog posebnog područja govori i činjenica da je u Strategiji nacionalne sigurnosti Republike Hrvatske posebno poglavlje posvećeno kibernetičkoj sigurnosti. Osnovno stajalište o važnosti ovog područja je: „Razvoj informacijskih i komunikacijskih tehnologija omogućio je procese koji povezuju svijet i olakšavaju život, ali je stvorio i nove prijetnje i rizike. Ovisnost društava i pojedinaca o internetu i informacijskoj tehnologiji predstavljaju posebnu osjetljivost. Napadi u kibernetičkom prostoru, bez obzira na motive, sve više ugrožavaju pojedince, organizacije i države. Istodobno, organizacijska fluidnost, geografska rasprostranjenost, tehnološka difuznost i neograničena mogućnost komunikacije otežavaju identifikaciju napadača, njihovih namjera i sposobnosti. Kibernetički kriminal je u porastu, a kibernetički prostor sve se više koristi za nezakonito djelovanje. Osim moguće povrede sigurnosti klasificiranih, osobnih i osjetljivih podataka, prijetnju predstavlja i korištenje kibernetičkog prostora za izazivanje žrtava i šteta u materijalnom svijetu. Radikalne ideje i pokreti, koji prerastaju u ekstremizam i terorizam, multipliciraju se i šire na internetu i društvenim mrežama, čime poprimaju doseg i utjecaj kakav ranije nisu imali.“ Strategija nacionalne sigurnosti Republike Hrvatske (Narodne novine, br. 73/17).

Distribucija kaznenih djela izvršena je podjelom na: a) kaznena djela kod kojih računalo, odnosno računalni sustavi služe kao sredstvo počinjeno kaznenog djela u odnosu na objekt zaštite; b) kaznena djela kod kojih se štiti poseban interes; c) kaznena djela računalnog kriminaliteta („prava“ kaznena djela računalnog kriminaliteta koja su izdvojena u zasebnu cjelinu; o tome i: Škrtić, D., dostupno na: https://www.fvv.um.si/dv2012/zbornik/informacijska_varnost/skrtic.pdf; Škrtić, D. (2011); Kokot, I. (2014)).

## 2.1. Kaznena djela kod kojih računalo, odnosno računalni sustavi služe kao sredstvo počinjeno kaznenog djela u odnosu na objekt zaštite

Kod ovih kaznenih djela računalo, odnosno računalni sustavi služe kao sredstvo počinjenja kaznenog djela. To su kaznena djela: Uvrede (čl. 147. KZ RH), Sramoćenja (čl. 148. KZ RH) i Klevete (čl. 149. KZ RH) navedena u Glavi XV: kaznenih djela protiv časti i ugleda.

Zakon predviđa strože kažnjavanje zbog načina počinjenja kaznenih djela kojim je „uvredljiv sadržaj" postao dostupan većem broju osoba.

Zatim javno poticanje na nasilje i mržnju (čl. 325. KZ RH) navedeno u Glavi XXX: kaznenih djela protiv javnog reda i mira. Javno poticanje na nasilje i mržnju uređeno je u KZ RH i zbog potrebe implementacije Okvirne odluke 2008/91/JHA o suzbijanju određenih oblika i načina izražavanja rasizma i ksenofobije putem kaznenog prava od 28. studenog 2008. godine (o nekim pitanjima zlouporabe društvenih mreža vidi: Roksandić Vidlička, S., Mamić, K. (2018)).

U ovu grupu kaznenih djela uvrštavamo i kaznena djela iz Glave XXVII: Kaznena djela zaštite intelektualnog vlasništva, jer prema načinima počinjenja obuhvaćaju i počinjenje pomoću računalnih sustava. To su kaznena djela: Povreda osobnih prava autora ili umjetnika izvođača (čl. 284. KZ RH), Nedozvoljena uporaba autorskog djela ili izvedbe umjetnika izvođača (čl. 285. KZ RH), Povreda drugih autorskom srodnih prava (čl. 286. KZ RH), Povreda prava na izum (čl. 287. KZ RH), Povreda žiga (čl. 288. KZ RH), Povreda registrirane oznake podrijetla (čl. 289. KZ RH). Kaznena djela su usklađena s čl. 10 Konvencije o kibernetičkom kriminalu te ih posebno određuje kao specifična kaznena djela zaštite intelektualnog vlasništva.

## 2.2. Kaznena djela kod kojih se štiti poseban interes

U ova kaznena djela KZ RH uvrstio je: Iskorištavanje djece za pornografiju (čl. 163. KZ RH), Iskorištavanje djece za pornografske predstave (čl. 164. KZ RH), Upoznavanje djece s pornografijom (čl. 165. KZ RH) i teška kaznena djela spolnog zlostavljanja i iskorištavanja djeteta (čl. 166. KZ RH) iz Glave XVII: kaznena djela spolnog zlostavljanja i iskorištavanja djeteta. Tu su i kaznena djela iz Glave XVIII: kaznena djela protiv braka, obitelji djece i to kazneno djelo povrede privatnosti djeteta (čl. 178. KZ RH).

Kod kaznenog djela opisanog u čl. 163. KZ RH novina je inkriminiranje svjesnog pristupanja putem informacijsko komunikacijskih tehnologija bilo kakvim materijalima pornografskog sadržaja. Dakle nije potrebno da osoba spremi te podatke na svoje računalo – u tom slučaju radilo bi se o posjedovanju, već kazneno djelo postoji i kad osoba samo privremeno pristupa i gleda pornografske materijale. Uz prikazivanje prave djece inkriminira se i realno prikazivanje nepostojeće djece te prikazivanje osoba koje izgledaju mlađe od 18 godina iako to nisu. Uz čl. 9. Konvencije o kibernetičkom kriminalu ovakva ponašanja zabranjuje i čl. 20. Konvencije Vijeća Europe o zaštiti djece od spolnog zlostavljanja i spolnog iskorištavanja[44].

[44] (https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=090000168046e1d1)

Zatim u čl. 164. KZ RH kažnjavaju se aktivnosti kojima se angažiraju djeca za sudjelovanje u pornografskim predstavama, zarađivanje na istima te gledanje pornografskih predstava u skladu sa čl. 21. Konvencije Vijeća Europe o zaštiti djece od seksualnog iskorištavanja i zlostavljanja. Kod kaznenog djela opisanog u čl. 165. KZ RH potrebno je spomenuti da je dobna granica je petnaest godina, a inkriminira se prodaja, poklanjanje, prikazivanje ili javno izlaganje, posredstvom računalnog sustava, mreže ili medija za pohranu računalnih podataka ili na drugi način činjenje pristupačnim spisa, slika, audiovizualnog sadržaja ili drugih predmeta pornografskog sadržaja ili prikazivanje pornografske predstave. Temeljnu, polaznu definiciju pornografije dao je Ustavni sud u svojoj odluci broj U-III-279/1998 od 9. listopada 1998. ali je ona za potrebe članka 165. KZ RH proširena. U odluci Ustavnog suda se navodi: „Tako kao orijentacijske točke mogu poslužiti slijedeće odrednice: namjena pornografije jest zadovoljenje nekog seksualnog interesa, njezin je pojavni oblik eksplicitno pokazivanje nekog seksualnog ponašanja na nizak, uvredljiv ili ponižavajući način, a karakteristično je da je lišena i svake političke, umjetničke ili znanstvene vrijednosti i poruke. Pri tome valja naglasiti stajalište ovog Suda kako karakter, namjena i orijentacija određene tiskovine u načelu ne može predstavljati alibi, odnosno okolnost koja bi ekskulpirala od odgovornosti za promicanje pornografije. Međutim, to onda kada se zaista nedvojbeno radi o pornografiji, odnosno kada je namjera ili postignuti efekt onog što se prikazuje – poticanje seksualnog nagona eksplicitnim pokazivanjem nekog seksualnog ponašanja.“ Odluka Ustavnog suda Republike Hrvatske broj U-III-279/1998 od 9. listopada 1998. (Narodne Novine br. 134/98). Članak 178. KZ RH usklađen je sa čl. 16. Konvencije o pravima djeteta (Narodne novine – Međunarodni ugovori, br. 12/93 i 20/97), koje određuje da dijete ima pravo na zakonsku zaštitu protiv samovoljnog ili nezakonitog miješanja u njegovu privatnost, obitelj, dom ili dopisivanje te nezakonitih napada na njegovu čast i ugled. Zaštita privatnosti odnosi se na svu djecu, a ne samo onu koja su mlađa od 14 godina te napisi u medijima moraju zaštiti identitet, odnosno prikriti identitet djeteta radi neprepoznavanja, "iznošenje ili prenošenje nečega iz osobnog ili obiteljskog života" što se odnosi na činjenične tvrdnje čija se istinitost ili neistinitost ne može dokazivati, uvedeni su i objavljivanje fotografija te otkrivanje identiteta djeteta suprotno propisima. Članak 1. Konvencije o pravima djeteta određuje da je dijete svako ljudske biće mlađe od 18 godina, osim iznimno, punoljetnost ne stječe ranije prema zakonima neke države.

## 2.3. Kaznena djela računalnog kriminaliteta

Računalni sustav je svaka naprava ili skupina međusobno spojenih ili povezanih naprava, od kojih jedna ili više njih na osnovi programa automatski obrađuju podatke, kao i računalni podaci koji su u njega spremljeni, obrađeni, učitani ili preneseni za svrhe njegovog rada, korištenja, zaštite i održavanja (čl. 87. st. 17. KZ RH). Računalni program je skup računalnih podataka koji su u stanju prouzročiti da računalni sustav izvrši određenu funkciju (čl. 87. st. 19. KZ RH), a računalni podatak je svako iskazivanje činjenica, informacija ili zamisli u obliku prikladnom za obradu u računalnom sustavu. (čl. 87. st. 18. KZ RH).

Ova kaznena djela normirana su u Glavi XXV: Kaznena djela protiv računalnih sustava, programa i podataka. Kaznena djela su: Neovlašteni pristup (čl. 266. KZ RH), Ometanje rada računalnog sustava (čl. 267. KZ RH), Oštećenje računalnih podataka (čl. 268. KZ RH); Neovlašteno presretanje računalnih podataka (čl. 269. KZ RH), Računalno krivotvorenje (čl. 270. KZ RH), Računalna prijevara (čl. 271. KZ RH), Zloporaba naprava (čl. 272. KZ RH) i teška kaznena djela protiv računalnih sustava, programa i podataka (čl. 273. KZ RH).

Kaznena djela su usklađena sa Konvencijom o kibernetičkom kriminalu. Specifičnost njihova počinjenja je da se čine u međunarodno javno dostupnom sustavu računala. Sukladno Konvenciji o kibernetičkom kriminalu postoje četiri grupe kaznenih djela: protiv tajnosti, nepovredivosti i dostupnosti podataka spremljenih na računalima i računalnih sustava; računalne prijevare i krivotvorenje uz pomoć računala; povrede i napadi na sadržaje i podatke na računalima; distribucija i širenje dječje pornografije i kaznena djela povrede autorskih i srodnih prava (usporedi: Pavlović, Š. Kazneni zakon (2013); Pavlović, Š. (2003).; Škrtić, dostupno na: https://www.fvv.um.si/dv2012/zbornik/informacijska_varnost/skrtic.pdf; Škrtić, D. (2011); Kokot, I. (2014)).

### 2.3.1. Neovlašteni pristup (čl. 266. KZ RH)

Inkriminira se nezakonit pristup tuđem računalnom sustavu, te računalnim podacima. Neovlašteni pristup jest pristup bez odobrenja. Razlog za sankcioniranje neovlaštenog pristupa je taj što je njegova realizacija najčešće preduvjet za činjenje nekog težeg kaznenog djela. Osnovni oblik kaznenog djela progoni se po prijedlogu, a kažnjiv je i pokušaj. Djelo je usklađeno sa čl. 2. Konvencije o kibernetičkom kriminalu. Naime, Zakon o kaznenom postupku Republike Hrvatske (u daljnjem tekstu ZKP RH) propisuje da se kaznena djela mogu progoniti: po prijedlogu; privatnom tužbom i po službenoj dužnosti. Progon po prijedlogu može dati ovlaštena fizička ili pravna osoba, kao i žrtva kaznenog djela. Progon se podnosi državnom odvjetniku, a daljnje postupanje državnog odvjetnika isto je kao i kod kaznenih djela za koje se progon poduzima po službenoj dužnosti. Vidi čl. 47. ZKP RH (NN 152/08, 76/09, 80/11, 91/12 - Odluka i Rješenje USRH, 143/12, 56/13, 145/13, 152/14 i 70/17). Tko s namjerom da počini kazneno djelo poduzme radnju koja prostorno i vremenski neposredno prethodi ostvarenju bića kaznenog djela, kaznit će se za pokušaj ako se za kazneno djelo može izreći kazna zatvora od pet godina ili teža kazna ili zakon izričito propisuje kažnjavanje i za pokušaj (čl. 34. st. 1. KZ RH).

### 2.3.2. Ometanje rada računalnog sustava (čl. 267. KZ RH)

Inkriminira se ometanje rada računalnog sustava, računalnih podataka ili programa te računalne komunikacije na način da se ovlaštenim korisnicima onemogući nesmetano korištenje njegovih resursa ili međusobna komunikacija. Ne mora ugroziti integritet ili tajnost podataka koji se nalaze unutar sustava. Radnja kaznenog djela čini se prenošenjem, oštećivanjem, brisanjem, kvarenjem, mijenjanjem ili činjenjem neupotrebljivim

računalnih podataka. Kazneno djelo usklađeno je s čl. 5. Konvencije o kibernetičkom kriminalu. Prema dostupnim analizama i podacima o ovom kaznenom djelo može se istaknuti da su počinitelji najčešće profesionalci koji iz različitih motiva ometaju rad računalnih sustava (vidi: Pavlović, Š. (2013); Šimundić, S., Franjić, S., Vdovjak, K. (2012); Bača, M., Ćosić, J. (2013)).

### 2.3.3. Oštećenje računalnih podataka (čl. 268. KZ RH)

Inkriminiraju se sve one radnje kojima se neovlašteno zadire u cjelovitost računalnih podataka ili programa, pri čemu nije važno je li im počinitelj neposredno pristupio ili je to učinio npr. izradom i prijenosom nekog malicioznog programa. Djelo je usklađeno sa čl. 4. Konvencije o kibernetičkom kriminalu i s čl. 4. Okvirne odluke 2005/222/JHA od 24. veljače 2005. godine (Okvirne odluke 2005/222/JHA od 24. veljače 2005. godine zamijenjena je Direktivom 2013/40/EU Europskog parlamenta i Vijeća od 12. kolovoza 2013. o napadima na informacijske sustave i o zamjeni Okvirne odluke Vijeća 2005/222/PUP, dostupno na:
https://eur-lex.europa.eu/legal-content/HR/TXT/HTML/?uri=LEGISSUM:l33193&from=HR).

### 2.3.4. Neovlašteno presretanje računalnih podataka (čl. 269. KZ RH)

Inkriminira se neovlašteno presretanje komunikacije prema računalnom sustavu, iz njega ili unutar njega odnosno između udaljenih računalnih sustava, njihovo snimanje, te činjenje takvih podataka dostupnim trećim osobama. Djelo je usklađeno sa čl. 3. Konvencije o kibernetičkom kriminalu. Smisao ove inkriminacije je u zaštiti nejavne komunikacije. Činjenjem ovog kaznenog djela povređuje se ili ugrožava pravo na poštovanje privatnog života, štiti se i pravo na uspostavljanje i razvijanje slobodne komunikacije (o pravu na poštovanje privatnog i obiteljskog života, doma i dopisivanja vidi: Vodič kroz članak 8. Europske konvencije o ljudskim pravima, dostupno na: https://uredzastupnika.gov.hr/UserDocsImages//dokumenti/Edukacija//Vodi%C4%8D%20kroz%20%C4%8Dlanak%208.%20Konvencije.pdf; Turkalj, K., Leppee Pažanin, D. (2018)).

### 2.3.5. Računalno krivotvorenje (čl. 270. KZ RH)

Inkriminira se krivotvorenje računalnih isprava zbog njihove važnosti u pravnom prometu i poslovanju. Kaznenim djelom pruža se zaštita vjerodostojnosti računalnih podataka u odnosu na sastavljača i sadržaj (vidi: Škrtić, D. dostupno na: https://www.fvv.um.si/dv2012/zbornik/informacijska_varnost/skrtic.pdf; Jelenski, M., Šuperina, M., Budiša, J. (2013); Casey E. Digital evidence and computer crime, Academis Press (2011)). Djelo je usklađeno s čl. 7. i 19. Konvencije o kibernetičkom kriminalu.

### 2.3.6. Računalna prijevara (čl. 271. KZ RH)

Vuletić i Nedić (2014: 680 i 683) navode da se radnja ovog kaznenog djela sastoji u manipulaciji s računalnim podacima ili programima, pri čemu se djeluje s namjerom stjecanja protupravne imovinske koristi. Ovo kazneno djelo je najučestalije u grupi računalnih kaznenih djela, a počinitelji žrtve su vrlo često iz različitih zemalja.

Postoje dva moguća shvaćanja prijevare. Prva je tzv. izravna računalna prijevara koja se sastoji u obmanjivanju žrtve, a kao sredstvo počinjenja kaznenog djela koristi se računalni sustav. Drugo shvaćanje je tzv. neizravna računalna prijevara koja se sastoji u varanju računalnog sustava. Objekt napada, „žrtva" je sam računalni sustav a onda posljedično i neka pravna ili fizička osoba. Kod ovog počinjenja neće doći do posljedičnog oštećenja neke osoba ako počinitelj prvo ne prevari računalni sustav. Vuletić i Nedić (2014) kao tipičan primjer ove prijevare navode uporabu tuđe bankovne kartice, gdje počinitelj podiže novac na bankomatu varajući računalni sustav a onda posljedično i osobu (fizičku ili pravnu) (vidi i: Sokanović, L., Orlović, A. (2017); Novoselec, P., Bojanić, I. (2007)). Djelo je usklađeno s čl. 8. i 19. Konvencije o kibernetičkom kriminalu.

### 2.3.7. Zloporaba naprava (čl. 272. KZ RH)

Ovim se djelom propisuje kažnjivost za pripremnu radnju poduzetu radi ostvarivanja nekog od navedenih djela. Radnja kaznenog djela sastoji se prvenstveno u izradi i/ili distribuciji različitih uređaja, računalnih programa ili podataka koji služe počinjenju nekog od kompjutorskih kaznenih djela. Takvi su uređaji za računalno krivotvorenje ili neovlašteno presretanje komunikacije, računalni programi za izradu malicioznih programa i sl. (vidi i: Dragičević, D. (2011)). To su i podaci koji počinitelju mogu poslužiti da ostvari neovlašteni pristup tuđem računalnom sustavu, poput neovlašteno pribavljenih korisničkih imena i lozinki ili pak uputa kako počiniti neko drugo kompjutorsko kazneno djelo. Odgovornost za ovo djelo uvjetuje se postojanjem namjere da se počini neko od navedenih djela kako se zbog posjedovanja takvih naprava ne bi kažnjavalo one koji ih imaju i koriste u legalne svrhe kao npr. u slučaju ovlaštenog ispitivanja ili zaštite računalnog sustava ili izrade efikasnih mjera i sredstava zaštite. „Naprava" se odnosi na bilo koji uređaj, dio ili komponentu vezanu uz računalo te sam računalni program kojim se čini radnja kaznenog djela. Radnja djela može se odnositi i na računalne zaporke, šifre ili druge podatke kojima se može pristupiti računalnim sustavima kako bi se njihovom uporabom počinilo kazneno djelo. Kazneno djelo je usklađeno s čl. 6. Konvencije o kibernetičkom kriminalu.

### 2.3.8. Teška kaznena djela protiv računalnih sustava, programa i podataka (čl. 273. KZ RH)

Kao teška kaznena djela određena su ona koja se čine putem tiska, radija, televizije, računalnog sustava ili mreže, na javnom skupu ili na da se drugi način javno potiče ili javnosti učini dostupnim letke, slike ili druge materijale kojima se poziva na nasilje ili mržnju

usmjerenu prema skupini ljudi ili pripadniku skupine zbog njihove rasne, vjerske, nacionalne ili etničke pripadnosti, podrijetla, boje kože, spola, spolnog opredjeljenja, rodnog identiteta, invaliditeta ili kakvih drugih osobina. Djelo čini i onaj tko javno odobrava, poriče ili znatno umanjuje kazneno djelo genocida, zločina agresije, zločina protiv čovječnosti ili ratnog zločina, usmjereno prema skupini ljudi ili pripadniku skupine zbog njihove rasne, vjerske, nacionalne ili etničke pripadnosti, podrijetla ili boje kože, na način koji je prikladan potaknuti nasilje ili mržnju protiv takve skupine ili pripadnika te skupine. Pokušaj kaznenog djela je kažnjiv.

## 3. Statistički pokazatelji stanja prijavljenih i razriješenih pojedinih kaznenih djela računalnog kriminaliteta u Republici Hrvatskoj

U tablici koja slijedi prikazana je prijavljivanost i razriješenost 7 kaznenih djela računalnog kriminaliteta za razdoblje od 2014. do 2018. godine na području Republike Hrvatske. Iz prikazanih podataka vidljivo je kako je u svim promatranim godinama daleko više prijavljivano kazneno djelo Računalne prijevare. U 2014. godine nakon kaznenog djela Računalne prijevare po čestini prijavljivanosti slijedi kazneno djelo Računalnog krivotvorenja, a potom slijedi podjednaka prijavljivanosti kaznenog djela Zlouporabe naprava i Neovlaštenog pristupa. Slični podaci se pronalaze i u 2015. i 2018. godini. U 2017. godini nakon kaznenog djela Računalne prijevare po prijavljivanosti slijedi kazneno djelo Računalnog krivotvorenja, a nakon njih kazneno djelo Ometanje rada računalnog sustava. Za razliku od navedenih godina u 2016. godini, nakon kaznenog djela Računalne prijevare po čestini prijavljivanosti slijedi Zlouporaba naprava i Neovlašteni pristup te tek na četvrtom mjestu Računalno krivotvorenje. Također, iz podataka prikazanih u Tablici 1. vidljiva je relativno visoka razriješenost gotovo svih prijavljenih kaznenih djela. Od prikazanih podataka potrebno je spomenuti kako je kod kaznenog djela Računalnog krivotvorenja u 2015. i 2018. godini zabilježena razriješenost veća od 100% što zapravo ukazuje da su policijskih službenici u tim godinama razriješili i nekoliko kaznenih djela koja su prijavljena u ranijim izvještajnim razdobljima odnosno godinama.

**Tablica 1**: Statistički pokazatelji prijavljenih i razriješenih pojedinih kaznenih djela računalnog krivotvorenja u Republici Hrvatskoj za razdoblje od 2014. do 2018. godine

| Kazneno djelo | 2014 Prijavljeno/ razriješeno | | 2015 Prijavljeno/ razriješeno | | 2016 Prijavljeno/ razriješeno | | 2017 Prijavljeno/ razriješeno | | 2018. Prijavljeno/ razriješeno | |
|---|---|---|---|---|---|---|---|---|---|---|
| Neovlašteni pristup (čl. 266. KZ RH) | 16 | 13 | 29 | 21 | 115 | 110 | 7 | 5 | 16 | 13 |
| | 100% | 81,2% | 100% | 72,4% | 100% | 95,7% | 100% | 71,4% | 100% | 81,3% |
| Ometanje rada računalnog sustava (čl. 267. KZ RH) | 1 | 1 | 2 | 2 | 4 | 2 | 11 | 10 | 1 | 1 |
| | 100% | 100% | 100% | 100% | 100% | 50% | 100% | 90,9% | 100% | 100% |
| Oštećenje računalnih podataka (čl. 268. KZ RH) | 4 | 4 | 7 | 3 | 6 | 2 | 7 | 7 | - | - |
| | 100% | 100% | 100% | 42,8% | 100% | 33,3% | 100% | 100% | 0% | 0% |
| Neovlašteno presretanje računalnih podataka (čl. 269. KZ RH) | 3 | 3 | 5 | 4 | 1 | 1 | 1 | - | - | - |
| | 100% | 100% | 100% | 80% | 100% | 100% | 100% | 0% | 0% | 0% |
| Računalno krivotvorenje (čl. 270. KZ RH) | 169 | 169 | 80 | 82 | 52 | 51 | 37 | 35 | 32 | 39 |
| | 100% | 100% | 100% | 102,5% | 100% | 98,1% | 100% | 94,6% | 100% | 121,9% |
| Računalna prijevara (čl. 271. KZ RH) | 960 | 864 | 1361 | 1215 | 1365 | 1238 | 1114 | 915 | 1310 | 1162 |
| | 100% | 90% | 100% | 89,3% | 100% | 90,7% | 100% | 82,1% | 100% | 88,7 |
| Zlouporaba naprava (čl. 272. KZ RH) | 19 | 18 | 69 | 69 | 160 | 157 | 9 | 7 | 17 | 17 |
| | 100% | 94,7% | 100% | 100% | 100% | 98,1% | 100% | 77,8% | 100% | 100% |

Izvor: Statistički pregled temeljnih sigurnosnih pokazatelja i rezultata rada u 2018., 2017. i 2015. godini (Ministarstvo unutarnjih poslova, Glavno tajništvo sektor za pravne poslove i strateško planiranje, služba za strateško planiranje, statistiku i unaprjeđenje rada, Statistički pregled temeljnih sigurnosnih pokazatelja i rezultata rada u 2018. godini, dostupno na:https://mup.gov.hr/UserDocsImages/statistika/2019/Pregled%20sigurnosnih%20pokazatelja%20u%202018%20godini/Statisticki%20pregled%202018_web.pdf, str. 56., Ministarstvo unutarnjih poslova, Glavno tajništvo sektor za pravne poslove i strateško planiranje, služba za strateško planiranje, statistiku i unaprjeđenje rada, Statistički pregled temeljnih sigurnosnih pokazatelja i rezultata rada u 2017. godini, dostupno na: https://mup.gov.hr/UserDocsImages/statistika/2018/Travanj/Statisticki%20pregled%202017.pdf, str. 48, Ministarstvo unutarnjih poslova, Glavno tajništvo sektor za pravne poslove i strateško planiranje, služba za strateško planiranje, statistiku i unaprjeđenje rada, Statistički pregled temeljnih sigurnosnih pokazatelja i rezultata rada u 2015. godini, dostupno na: https://mup.gov.hr/UserDocsImages/statistika/2016/Statistika_2015_nova..pdf, str. 42.)

U Tablici 2. prikazan je ukupan broj kaznenih djela i broj prijavljenih kaznenih djela računalnog kriminaliteta za razdoblje od 2014. do 2018. godine u Republici Hrvatskoj. Kaznena djela računalnog kriminaliteta prikazana u Tablici 2. ovog rada podrazumijevaju

prijavljena kaznena djela koja su prikazana u Tablici 1. ovog rada. Ukupan broj kaznenih djela obuhvaća i kaznena djela za koja se progon poduzima po službenoj dužnosti, ali i kaznena djela po privatnoj tužbi i izostanku prijedloga. Kod ukupnog broja kaznenih djela u promatranom razdoblju vidljiv je konstantan pad evidentiranih kaznenih djela. Za razliku od ukupnog broja kaznenih djela kod kaznenih djela računalnog kriminaliteta vidljive su značajne oscilacije u ukupnom broju prijavljenih kaznenih djela prikazanih u Tablici 1.

Naime, u periodu od 2014. do 2016. godine iz godine u godinu zabilježen je porast prijavljenih kaznenih djela računalnog kriminaliteta. U 2017. godine u odnosu na 2016. godinu zabilježen je pad broja prijavljenih kaznenih djela računalnog kriminaliteta za 30,4 % dok je u 2018. godini u odnosu na 2017. godinu zabilježen porast prijavljenih kaznenih djela računalnog kriminaliteta za 16 %.

Ukoliko se u pojedinačnim godinama pogleda udio prijavljenog računalnog kriminaliteta u ukupnom broju kaznenih djela u pojedinoj godini vidljivo je kako je relativno najveći udio računalnog kriminaliteta u ukupnom broju kaznenih djela u 2016. godini (2%), potom slijedi 2018. godina s 1,7 % te 2015. godina s 1,63 %.

To ukazuje na potrebu stalne edukacije korisnika različitih sustava temeljem kojih se čine ova kaznena djela te prevencije i jačanja svijesti. To je jednim dijelom bila i osnova istraživanja čije rezultate prikazujemo u sljedećem poglavlju.

**Tablica 2.** Ukupan broj kaznenih djela i broj prijavljenih kaznenih djela računalnog kriminaliteta za razdoblje od 2014. do 2018. godine u Republici Hrvatskoj

| Godina | 2014 | | 2015 | | 2016 | | 2017 | | 2018 | |
|---|---|---|---|---|---|---|---|---|---|---|
| Ukupno k.d. | 96877 | 100% | 95037 | 100% | 85620 | 100% | 83047 | 100% | 78922 | 100% |
| K. d. računalnog krim. | 1172 | 1,2% | 1553 | 1,63% | 1703 | 2% | 1186 | 1,4% | 1376 | 1,7% |

Izvor: Statistički pregled temeljnih sigurnosnih pokazatelja i rezultata rada u 2018., 2017. i 2015. godini (Ministarstvo unutarnjih poslova, Glavno tajništvo sektor za pravne poslove i strateško planiranje, služba za strateško planiranje, statistiku i unaprjeđenje rada, Statistički pregled temeljnih sigurnosnih pokazatelja i rezultata rada u 2018. godini, dostupno na: https://mup.gov.hr/UserDocsImages/statistika/2019/Pregled%20sigurnosnih%20pokazatelja%20u%202018%20godini/Statisticki%20pregled%202018_web.pdf, str. 1., Ministarstvo unutarnjih poslova, Glavno tajništvo sektor za pravne poslove i strateško planiranje, služba za strateško planiranje, statistiku i unaprjeđenje rada, Statistički pregled temeljnih sigurnosnih pokazatelja i rezultata rada u 2017. godini, dostupno na:https://mup.gov.hr/UserDocsImages/statistika/2018/Travanj/Statisticki%20pregled%202017.pdf, str. 1, Ministarstvo unutarnjih poslova, Glavno tajništvo sektor za pravne poslove i strateško planiranje, služba za strateško planiranje, statistiku i unaprjeđenje rada, Statistički pregled temeljnih sigurnosnih pokazatelja i rezultata rada u 2015. godini, dostupno na: https://mup.gov.hr/UserDocsImages/statistika/2016/Statistika_2015_nova..pdf, str. 1)

## 4. Rezultati istraživanja o svjesnosti računalnog kriminaliteta

### 4.1. Cilj istraživanja

Ciljevi istraživanja o svjesnosti računalnog (*cyber*) kriminaliteta bili su:

- Utvrditi navike mladih vezane za korištenje interneta;
- Ispitati svijest i iskustva o opasnostima računalnog (cyber) kriminaliteta;
- Utvrditi razinu viktimizacije računalnim kriminalitetom;
- Utvrditi postoji li veza između negativnih iskustava na internetu te eventualne viktimizacije s promjenom ponašanja prilikom korištenja interneta;
- Usporediti statističke podatke o broju prijavljenih i razriješenih kaznenih djela sa rezultatima istraživanja.

### 4.2. Opis uzorka

Istraživanje je provedeno na uzorku od 344 ispitanika, studenata veleučilišta i visokih škola u Republici Hrvatskoj, a u samoj strukturi uzorka 55,5% ispitanika su muškarci te 44,5% žene. Svi ispitanici bili su stariji od 19 godina, a prosječna dob iznosila je 21,5 godine. Najveći dio ispitanika studenti su preddiplomskih studija (77%), zatim diplomskih studija (21,8%), a 1,2 % integriranih studija. U odnosu na područja u kojima studiraju 47,7% ispitanika studira na visokim učilištima iz područja društvenih znanosti, 30,8% tehničkih znanosti, 8,8% interdisciplinarnih znanosti te preostalih 12,7 % iz ostalih znanstvenih područja. Većina ispitanika (66,9%) su redovni studenti, a jedna trećina (33,1%) izvanredni.

### 4.3. Anketni upitnik

U ovom istraživanju korišten je anketni upitnik originalno objavljen i javno dostupan kao „Cyber crime awareness Survey“ (https://www.surveymonkey.com/r/WJGH7MH). Međutim, spomenuti upitnik, koji sadrži varijable kojima se ispituje svijest o opasnostima na internetu i negativno iskustvo ispitanika vezano za korištenje interneta, modificiran je i nadopunjen varijablama koje su konstruirali autori ovog istraživanja. Spomenute varijable odnose se na navike korištenja interneta, prijavljivanje policiji kaznenih djela na internetu i poduzimanje određenih radnji (preventivnih ponašanja) u korištenju interneta nakon negativnih iskustava na digitalnim mrežama. Modificirani upitnik sadrži 30 varijabli, uključujući i varijable kojima se ispituju socio-demografska obilježja ispitanika. Skale u upitniku su nominalnog tipa.

Samo ispitivanje studenata veleučilišta i visokih škola provedeno je putem on-line ankete, na način da je upitnik dostavljen njihovim matičnim ustanovama, koje su izvršile distribuciju prema studentima. S obzirom na način odabira uzorka i uvažavajući činjenicu da su u obradu uzeti odgovori onih ispitanika koji su ispunili dostavljeni im upitnik, može se konstatirati kako se radi o prigodnom uzorku.

## 4.4. Metode obrade rezultata

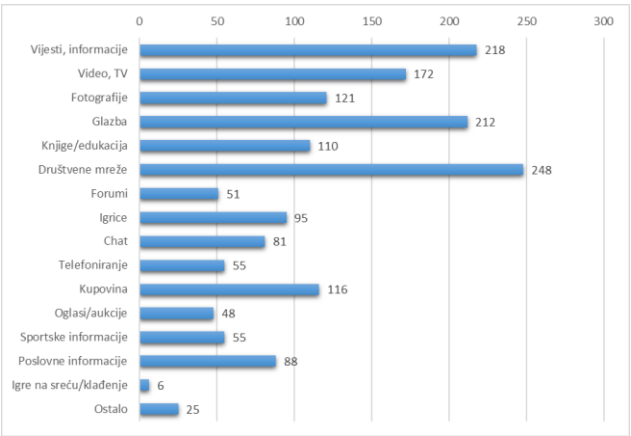
Rezultati dobiveni ovim istraživanjem obrađeni su u statističkom programu SPSS, a u radu su prikazani rezultati deskriptivne statistike, marginalne frekvencije odgovora ispitanika na pojedina pitanje. Radi utvrđivanja postojanja veza između negativnih iskustava na internetu te eventualne viktimizacije s promjenom ponašanja prilikom korištenja interneta korišten je hi-kvadrat test, kao test nezavisnosti dviju varijabli.

## 4.5. Rezultati istraživanja

Ovim istraživanjem ispitane su prije svega navike ispitanika vezane uz korištenje interneta. Dobiveni rezultati pokazuju da od uređaja koji ispitanici najčešće koriste je mobitel (67,4% ispitanika), zatim računalo (28,2%), dok svega 4,4% na prvome mjestu koristi neki drugi uređaj (televizor, tablet, radio i ostalo). Naravno, sukladno tome, internetu ispitanici najčešće pristupaju putem mobitela, to čini 74,4% njih, zatim putem prijenosnog računala 15,1% i stolnog računala 10,2%. Neznatan broj ispitanika internetu pristupa putem *smart* TV-a ili na druge načine. Također je interesantan podatak da studenti uključeni u istraživanje u 74,4% slučajeva internet najviše upotrebljavaju kod kuće, zatim u 21,8% na fakultetu ili poslu, a zatim 3,8% na javnom mjestu. Trećina ispitanika dnevno provede prosječno 4 sata na internetu, jedna petina više od 6 sati, a po jedna šestina 2 te 6 sati dnevno. Gotovo polovina ispitanika (46,8%) neprekidno je povezana s internetom, 27,6% internet najčešće korist navečer, 18,3% poslije podne, a 7,3 posto prije podne.

U grafikonu 1 prikazani su podaci o tome koje vrste sadržaja/aktivnosti na internetu ispitanike najviše interesiraju (ispitanicu su mogli odabrati više ponuđenih odgovora). Iz podataka je vidljiva najveća zastupljenost korištenja društvenih mreže (koristi ih 72% ispitanika), zatim pregledavanje vijesti i informacija (63% ispitanika), slušanje glazbe (62%), dok primjerice za kupovinu internet koristi 34% ispitanika itd.

Grafikon 1. Vrste sadržaja/aktivnosti na internetu koje ispitanike najviše interesiraju (N=344)

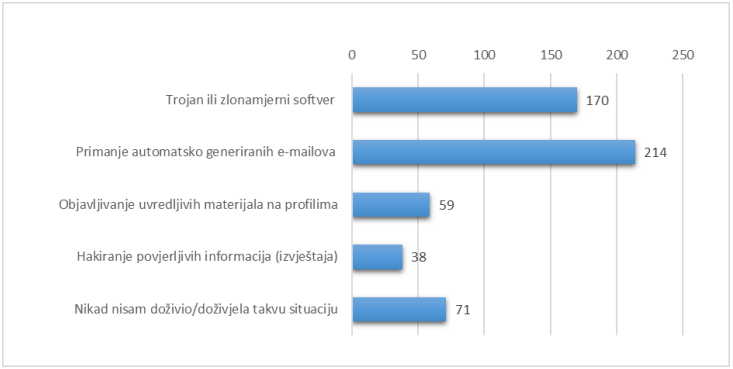



Prema dobivenim podacima velika većina ispitanika na računalu ima instaliran antivirusni program (89,8%), a njih 72,7% ima instaliran i podešen vatrozid (e*ng. Firewall*).

Nakon podataka o navikama ispitanika u vezi s korištenjem interneta, istraživanjem su prikupljeni i podaci o svjesnosti od opasnosti od računalnog kriminaliteta. Na pitanje: Koliko ste svjesni računalnog (*cyber*) kriminaliteta 43 % ispitanika odgovara da su jako dobro svjesni, 43,9 % da zna za to, a 13,1 % da i ne tako dobro. Najviše ispitanika (54,9%) svoje informacije na internetu ne doživljava sigurnima, za razliku od 33,4% njih koji ih doživljavaju sigurnima, a svega 7,8 % vrlo sigurnima, dok ostali nemaju stav o ovom pitanju. Čak 97,4 % ispitanika se slaže s tvrdnjom da je sigurnost na internetu nužna, a 94,4 % da je u vezi informacijske sigurnosti zaštita lozinke važna.

Na grafikonu 2. prikazani su podaci o negativnim iskustvima ispitanika na internetu. Vidljivo je kako je najučestalije primanje automatski generiranih e-mailova (doživjelo 62,2% ispitanika), a zatim trojan ili zlonamjerni softver (49,4% ispitanika). 20,6 % ispitanika nikada nije doživjelo neku od u istraživanju navedenih situacija.

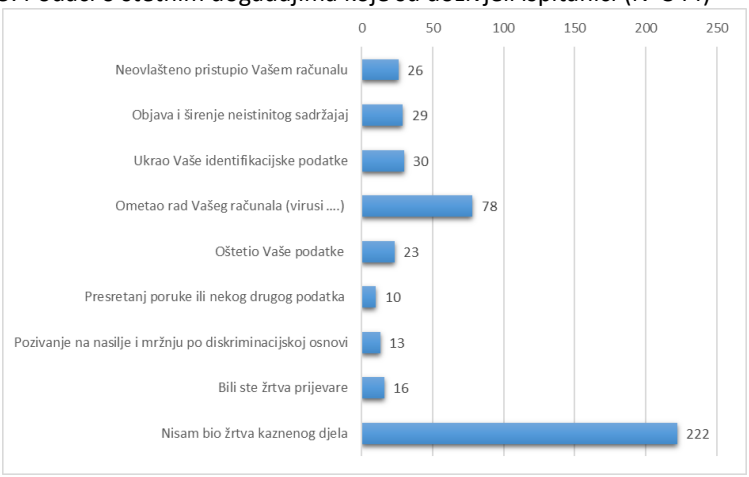
Grafikon 2. Podaci o negativnim iskustvima ispitanika na internetu (N=344)




Jedan od ciljeva istraživanja bio je i istražiti viktimizaciju povezanu s računalnim kriminalitetom te spremnost ispitanika na prijavljivanje kaznenog djela policiji. Podaci govore da od 344 ispitanika njih 18,4% su bili žrtve računalnog kriminaliteta. Ukoliko se ovaj podatak usporedi s ranijim istraživanjima u vezi s viktimizacijom u Hrvatskoj, može se zaključiti da je viktimizacija povezana s računalnim kriminalitetom puno veća nego viktimizacija drugim kaznenim djelima. Od ispitanika koji su bili žrtve kaznenog dijela većina ih je oštećena jedanput (54,6%), a 43,4 % dva ili više puta. Prema rezultatima Nacionalnog istraživanja javnog mnijenja o percepciji sigurnosti građana, postupanju policije te suradnji između policije i lokalne zajednice (GfK Croatia, 2009) dobivena je razina viktimizacije za pojedina kaznena dijela. Pa tako 3% ispitanika doživjelo je da im netko nasilno ili uz prijetnju nasilja nešto oteo ili pokušao oteti, 4 % da su bili žrtva krađe, 5% da su doživjeli provalu ili pokušaj provale u stan /kuću, 10 % da su bili prevareni, 7 % da su bili napadnuti ili im je netko prijetio napadom. U ovom istraživanju nije istraživana viktimizacija povezana s računalnim kriminalitetom.

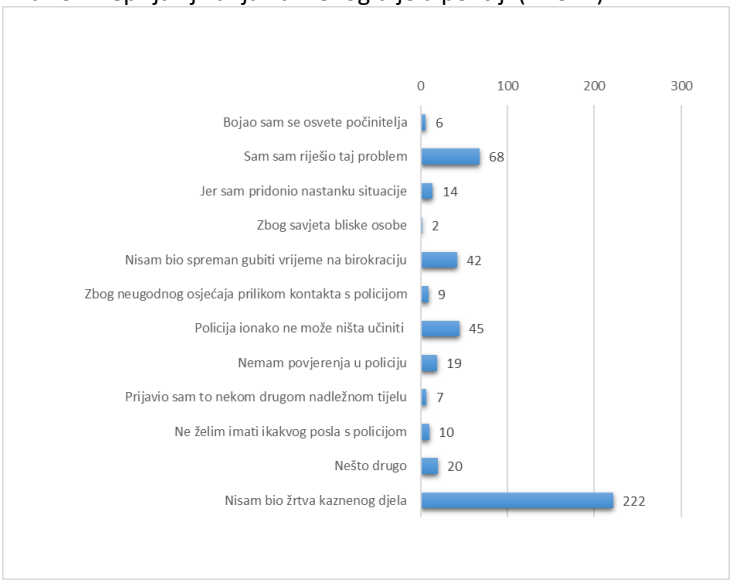
U grafikonu 3. prikazani su podaci o tome koje su štetne događaje doživjeli ispitanici iz ovog istraživanja. Iz podataka je razvidno da se štetni događaji najčešće odnose na ometanje rada računala putem zlonamjernih softvera (virusa), zatim krađu osobnih podataka, objavu i širenje neistinitih i štetnih sadržaja te neovlašteni pristup računalu. U 42,8 % slučajeva ispitanici oštećeni kaznenim dijelom računalnog kriminaliteta zna tko je počinitelj. Međutim, svega ih je 17% prijavilo to kazneno djelo.

Grafikon 3. Podaci o štetnim događajima koje su doživjeli ispitanici (N=344)



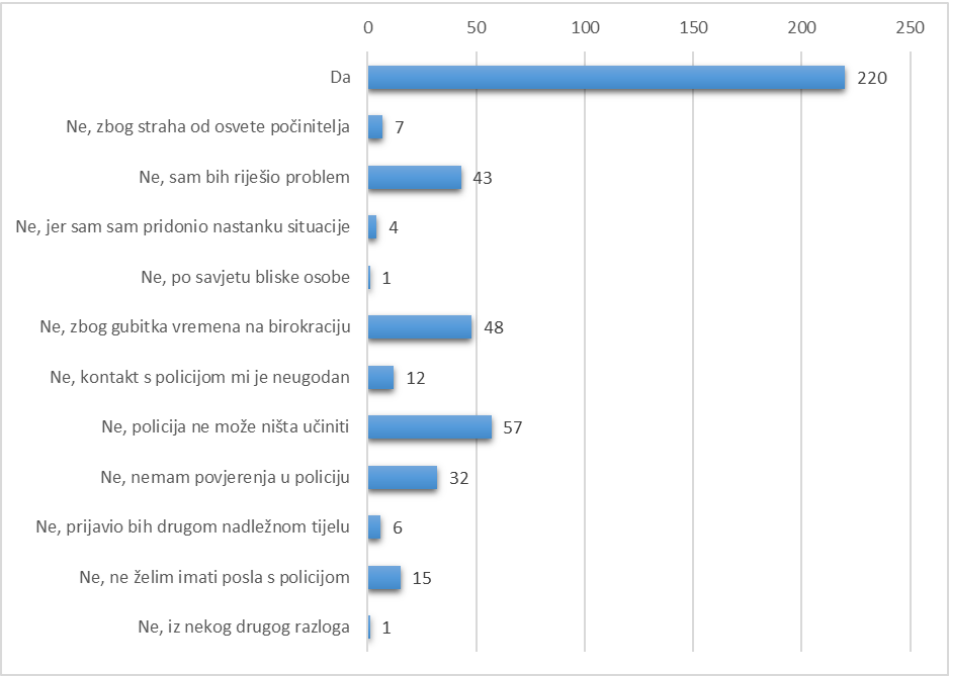

U grafikonu 4. prikazani su podaci o razlozima zbog kojih oštećeni ispitanici nisu prijavili kazneno djelo. Najčešće navedeni razlog je to što su ispitanici sami riješili taj problem, zatim nisu bili spremani gubiti vrijeme na birokraciju ili su smatrali da policija ionako ne može ništa učiniti (nemoćna je kod rješavanja takvog slučaja).

Grafikon 4. Razlozi neprijavljivanja kaznenog dijela policiji (N=344)




Za razliku od prethodnog pitanje u kojem je provjeravana reakcija na počinjeno kazneno djelo, u slijedećem pitanju napravljena je procjena spremnosti prijavljivanja računalnog kriminaliteta među svim ispitanicima, bez obzira na prethodno iskustvo (grafikon 5.).

Grafikon 5. Spremnost prijavljivanja računalnog kriminaliteta policiji (N=344)




Rezultati pokazuju da bi 64% ispitanika prijavilo djelo policiji, a od onih koji to ne bi učinili najviše je onih koji smatraju da policija ne može ništa učiniti (17%), zatim onih koji ne žele gubiti vrijeme na birokraciju (14%) ili koji bi sami riješili problem (13%).

Dobar pokazatelj viktimizacije putem računalnog kriminaliteta je i prouzročena materijalna šteta, tako da se jedna od varijabli u upitniku odnosila i na pitanje gubitka novca zbog ove vrste kriminaliteta. Prema dobivenim podacima 14,2% ispitanika pretrpjelo je materijalnu štetu. Međutim, na pitanje jesu li zbog toga prestali kupovati preko interneta većina ispitanika (60,2%) odgovara da kao mjeru koristi kupovinu isključivo preko provjerenih internetskih stranica, dok je 4,9% ispitanika donekle prestalo kupovati preko interneta.

Generalno gledajući, vezano uz sve probleme povezane s računalnim krminalitetom s kojima se ispitanici susreću na internetu, relativno je mali broj onih koji nisu ništa poduzeli (7,8%). Najviše je onih koji su prestali posjećivati nesigurne stranice (29,1%), zatim, onih koji su instalirali dodatnu zaštitu na svoj uređaj (21,2%), a mali broj onih koji su ugasili svoj račun na društvenoj mreži (6,3%).

Mišljenja ispitanika podijeljena su u oko tvrdnje da zakoni koji su na snazi mogu kontrolirati počinitelje računalnog kriminaliteta. Njih 60,8% ne slaže se s tom tvrdnjom,

24,4% ima neutralan stav (niti se slažu, niti se ne slažu), a svega 14,8% ispitanika ima pozitivno mišljenje, odnosno misli da su zakoni u tom smislu dobri.

Radi ispitivanja **povezanosti korištenja antivirusnog programa i doživljavanja kaznenog djela počinjenog preko računala**, korišten je hi-kvadrat test za dva nezavisna uzorka. Hi-kvadrat test nezavisnosti nije pokazao značajnu povezanost između posjedovanja antivirusnog programa na svom računalu i bivanja žrtvom kaznenog djela počinjenog preko računala, $\chi^2$ (1, n=344)= 0.205, p=0,651). Jednako tako hi-kvadrat test nezavisnosti nije pokazao značajnu povezanost između posjedovanja vatrozida (*eng: firewall*) na svom računalu i bivanja žrtvom kaznenog djela počinjenog preko računala, $\chi^2$ (2, n=344)= 2.453, p=0,293). Ovakav rezultat uvjetovan je činjenicom da velika većina ispitanika ima instaliran ili jedan ili oba oblika zaštite na svojim računalima, tako da se i nije mogla utvrditi statistički značajna razlika u odnosu na relativno mali broj onih koji ne koriste antivirusni program i/ili vartozid i bili su viktimizirani.

Jedan od ciljeva ovog istraživanja bio je i utvrditi postoji li veza između negativnih iskustava na internetu te eventualne viktimizacije putem računalne mreže s promjenom ponašanja prilikom korištenja interneta. Takva povezanost, na razini statističke značajnosti je potvrđena. Ovaj podatak pokazuje također razinu svijesti o opasnostima računalnog kriminaliteta te spremnost ispitanika na promjenu ponašanja radi smanjenja rizika i prevencije budućih kaznenih djela. U nastavku rada prikazana je povezanost **bivanja žrtvom kaznenog djela počinjenog preko računala i promjene ponašanja na internetu** utvrđena korištenjem hi-kvadrat test za dva nezavisna uzorka. Hi-kvadrat test nezavisnosti pokazuje značajnu povezanost **bivanja žrtvom kaznenog djela počinjenog preko računala i promjene ponašanja na internetu u pogledu**:

- **prestanka posjećivanja nesigurnih stranica**, $\chi^2$ (1, n=344)= 14,180, p<0,01). Utvrđena je niska do srednje visoka veličina učinka $\Phi$ (Fi) =0,21, p<0.01.
- **prestanka spajanja na internet preko nesigurne mreže**, $\chi^2$ (1, n=344)= 6,041, p=0,014). Utvrđena je niska veličina učinka $\Phi$ (Fi) =0,14, p<0.01.
- **brisanja računa na društvenim mrežama**, $\chi^2$ (1, n=344)= 7,065, p=0,003). Utvrđena je niska veličina učinka $\Phi$ (Fi) =0,159, p<0.01.
- **instaliranja dodatne zaštite za svoj uređaj**, $\chi^2$ (1, n=344)= 14,940, p<0,01). Utvrđena je niska do srednje visoka veličina učinka $\Phi$ (Fi) =0, 218, p<0.01.
- **poduzimanja nečega drugog zbog sigurnosti na internetu**, $\chi^2$ (1, n=344)= 24,100, p<0,01). Utvrđena je srednje visoka veličina učinka $\Phi$ (Fi) =0, 275, p<0.01.

Dobiveni rezultati potvrđuju da je negativno iskustvo na internetu i viktimizacija putem računalne mreže povezana s promjenama ponašanja korisnika i njihovim navikama u daljnjem korištenju interneta.

## 5. Zaključak

U samom zaključku ističemo nekoliko utvrđenih činjenica, a odnose se na stalno povećanje broja počinjenih kaznenih djela računalnog kriminaliteta, što je usko vezano uz načine obavljanja svakodnevnih ali i poslovnih aktivnosti. Nadalje, vidljiv je visoki postotak razjašnjenosti prijavljenih kaznenih djela, što je u suprotnosti s rezultatima ispitivanja gdje ispitanici iskazuju da iz različitih razloga ne bi prijavili kazneno djelo policiji. Nadalje, može se zaključiti da postoji tzv. tamna broja kriminaliteta te da se upravo ta „tamna broja“ kriminaliteta dovodi u vezu s padom ukupno prijavljenog kriminaliteta.

Za policiju je svakako važno područje u kojem se mogu postići značajni pomaci upravo jačanje prevencije i rada s potencijalnim žrtvama kako bi se stvorilo povjerenje između policije i građana (tamo gdje ne postoji) te otklonile zaprjeke za prijavljivanje kaznenih djela i suradnju tijekom istraživanja istih jer kako podaci pokazuju stupanj uspješnosti u razjašnjavanju prijavljenog kriminaliteta je vrlo visok, kao što je visok stupanj svjesnosti o opasnostima novih tehnologija ali relativno neadekvatna zaštita.

**LITERATURA:**

1. Bača, M., Ćosić, J. (2013). Prevencija računalnog kriminaliteta, Policija i sigurnost, 22/1, str. 146. – 158.
2. Casey E.: Digital evidence and computer crime, Academis Press, 2011.
3. Cyber crime awareness Survey, dostupno na: https://www.surveymonkey.com/r/WJGH7MH
4. Čizmić, J., Boban, M. (2017). Elektronički dokazi u sudskom postupku i računalna forenzička analiza, Zbornik Pravnog fakulteta u Rijeci, 38/1., str. 23. – 50.
5. Direktiva 2013/40/EU Europskog parlamenta i Vijeća od 12. kolovoza 2013. o napadima na informacijske sustave i o zamjeni Okvirne odluke Vijeća 2005/222/PUP, dostupno na: https://eur-lex.europa.eu/legal-content/HR/TXT/HTML/?uri=LEGISSUM:l33193&from=HR, pristupljeno 26.07.2019.
6. Dodatni protokol uz Konvenciju o kibernetičkom kriminalu o inkriminiranju djela rasističke i ksenofobne naravi počinjenih pomoću računalnih sustava, dostupno na: https://www.coe.int/en/web/conventions/full-list/-/conventions/rms/090000168008160f, pristupljeno 01.08.2019.
7. Dragičević, D. Kompjuterski kriminalitet i informacijski sustavi, IBS, Zagreb, 2004.
8. Jelenski, M., Šuperina, M., Budiša, J. (2013). Kriminalitet platnim karticama (krađa identiteta, krivotvorenje i zlouporaba platne kartice), Policija i sigurnost, 22/3, str. 372. – 395.
9. Kazneni zakon Republike Hrvatske, Narodne Novine, br. 125/11, 144/12, 56/15, 61/15, 101/17, 118/18.
10. Kokot I. (2014). Kaznenopravna zaštita računalnih sustava, programa i podataka, Zagrebačka pravna revija, 3/3. str. 303. – 330.
11. Konvencija o kibernetičkom kriminalu Vijeća Europe, dostupno na: https://www.coe.int/en/web/conventions/full-list/-/conventions/rms/0900001680081561, pristupljeno 01.08.2019.
12. Konvencije o pravima djeteta, Narodne novine – Međunarodni ugovori, br. 12/93 i 20/97.
13. Konvencije Vijeća Europe o zaštiti djece od spolnog zlostavljanja i spolnog iskorištavanja, https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=090000168046e1d1., pristupljeno: 26.07.2019.
14. Krapac, D. Kompjutorski kriminalitet: pregled glavnih pitanja krivičnopravne zaštite društvenih vrijednosti u postupcima elektronske obrade podataka, Pravni fakultet, Zagreb, 1992.
15. Ministarstvo unutarnjih poslova, Glavno tajništvo sektor za pravne poslove i strateško planiranje, služba za strateško planiranje, statistiku i unaprjeđenje rada, Statistički pregled temeljnih sigurnosnih pokazatelja i rezultata rada u 2018. godini, dostupno na:

https://mup.gov.hr/UserDocsImages/statistika/2019/Pregled%20sigurnosnih%20pokazatelja%20u%202018%20godini/Statisticki%20pregled%202018_web.pdf.

16. Ministarstvo unutarnjih poslova, Glavno tajništvo sektor za pravne poslove i strateško planiranje, služba za strateško planiranje, statistiku i unaprjeđenje rada, Statistički pregled temeljnih sigurnosnih pokazatelja i rezultata rada u 2017. godini, dostupno na: https://mup.gov.hr/UserDocsImages/statistika/2018/Travanj/Statisticki%20pregled%202017.pdf.
17. Ministarstvo unutarnjih poslova, Glavno tajništvo sektor za pravne poslove i strateško planiranje, služba za strateško planiranje, statistiku i unaprjeđenje rada, Statistički pregled temeljnih sigurnosnih pokazatelja i rezultata rada u 2015. godini, dostupno na: https://mup.gov.hr/UserDocsImages/statistika/2016/Statistika_2015_nova..pdf.
18. Nacionalno istraživanje javnog mnijenja o percepciji sigurnosti građana, postupanju policije te suradnji između policije i lokalne zajednice, GfK, Croatia, 2009, http://www.seesac.org/f/docs/SALW-Surveys/On-Citizen-Perception-of-Safety-and-Security-in-the-Republic-of-Croatia-BCMS.pdf, pristupljeno 30.07.2019.
19. Novoselec, P., Bojanić, I. Posebni dio kaznenog prava, Pravni fakultet Sveučilišta u Zagrebu, Zagreb, 2007.
20. Odluka Ustavnog suda Republike Hrvatske broj U-III-279/1998 od 9. listopada 1998, Narodne Novine br. 134/98.
21. Okvirna odluka 2008/91/JHA o suzbijanju određenih oblika i načina izražavanja rasizma i ksenofobije putem kaznenog prava od 28. studenog 2008. godine.
22. Pavlović, Š. Kazneni zakon, Libertin naklada, Rijeka, 2013.
23. Pavlović, Š. (2003). Kompjuterska kaznena djela u Kaznenom zakoniku – Osnove hrvatskog informacijskog kaznenog prava, Hrvatski ljetopis za kazneno pravo i praksu, 10/2, str. 625. – 664.
24. Roksandić Vidlička, S., Mamić, K. (2018). Zlouporaba društvenih mreža u javnom poticanju na nasilje i mržnju i širenju lažnih vijesti: potreba transplantiranja njemačkog zakona o jačanju provedbe zakona na društvenim mrežama?, Hrvatski ljetopis za kazneno pravo i praksu, 25/2, str. 329. – 357.
25. Sokanović, L., Orlović, A. (2017). Oblici prijevara u Kaznenom zakonu, Hrvatski ljetopis za kazneno znanosti i praksu, 24/2, str. 583. – 615.
26. Strategija nacionalne sigurnosti Republike Hrvatske, Narodne novine, br. 73/17.
27. Šimundić, S., Franjić, S., Vdovjak, K. (2012). HOAX, Zbornik radova Pravnog fakulteta u Splitu, 49/3, str. 459. – 480.
28. Škrtić, D. Kaznena djela računalnog kriminaliteta u novom Kaznenom zakonu RH, dostupno na: https://www.fvv.um.si/dv2012/zbornik/informacijska_varnost/skrtic.pdf, posjećeno 26.07.2019.
29. Škrtić, D. Kazneno pravna zaštita informatičkih sadržaja, Doktorska disertacija Sveučilište u Zagrebu, Pravni fakultet, 2011.

30. Turkalj, K., Leppee Pažanin, D. (2018). Izazovi pravnog uređenja zadržavanja podataka elektroničke komunikacije u svjetlu nedavne prakse suda EU-a, Godišnjak Akademije pravnih znanosti Hrvatske, IX/1, str. 141. – 173.
31. Vodič kroz članak 8. Europske konvencije o ljudskim pravima, dostupno na: https://uredzastupnika.gov.hr/UserDocsImages//dokumenti/Edukacija//Vodi%C4%8D%20kroz%20%C4%8Dlanak%208.%20Konvencije.pdf, pristupljeno 26.07.2019.
32. Vojković G., Štambuk-Sunjić M. (2006). Konvencija o Kibernetičkom kriminalu i Kazneni zakon republike Hrvatske, Zbornik radova Pravnog fakulteta u Splitu, str. 123 – 136.
33. Vuković, H. (2012). Kibernetska sigurnost i sustav borbe protiv kibernetskih prijetnji u Republici Hrvatskoj; Nacional security and the future, 13/3, str. 12.-31.
34. Vuletić, I. (2014). Primjenjivost tradicionalnih kaznenopravnih koncepata na računalni kriminal, Zbornik Pravnog fakulteta u Zagrebu, 64/5-6, str. 895. – 909.
35. Vuletić, I., Nedić, T. (2014). Računalna prijevara u hrvatskom kaznenom pravu, Zbornik Pravnog fakulteta u Rijeci, 35/2, str. 679. – 692.
36. Zakon o autorskom pravu i srodnim pravima, Narodne Novine br. 167/03, 79/07, 80/11, 141/13, 127/14, 62/17, 96/18.
37. Zakon o elektroničkoj ispravi, Narodne Novine, br.150/05.
38. Zakon o elektroničkom izdavanju računa u javnoj nabavi, Narodne Novine, br. 94/18.
39. Zakon o elektroničkom novcu, Narodne Novine, br. 64/18.
40. Zakon o elektroničkoj trgovini, Narodne Novine, br. 173/03, 67/08, 36/09, 130/11, 30/14, 32/19.
41. Zakon o informacijskoj sigurnosti, Narodne Novine, br. 79/07.
42. Zakona o izmjenama i dopunama Kaznenog zakona, Narodne novine, br. 105/04.
43. Zakon o kaznenom postupku Republike Hrvatske, Narodne Novine, br. 152/08, 76/09, 80/11, 91/12 - Odluka i Rješenje USRH, 143/12, 56/13, 145/13, 152/14 i 70/17.
44. Zakon o provedbi Opće Uredbe o zaštiti podataka, Narodne Novine br. 42/18.
45. Zakon o pravu na pristup informacijama, Narodne Novine br. 25/13, 85/15.
46. Zakon o tajnosti podataka, Narodne Novine br. 79/07, 86/12.
47. Zakon o provedbi Uredbe (EU) br. 910/2014 Europskog parlamenta i Vijeća od 23. srpnja 2014. o elektroničkoj identifikaciji i uslugama povjerenja za elektroničke transakcije na unutarnjem tržištu i stavljanju izvan snage Direktive 1999/93/EZ, Narodne Novine, br. 62/17.