FBIM Transactions

# RAČUNARSKA SABOTAŽA

## COMPUTER SABOTAGE

**Živanka Miladinović Bogavac**
Poslovni i pravni fakultet, Univerzitet „Union - Nikola Tesla“, Beograd, Srbija


JEL kategorija rada: **D82, G32, L86**

***Apstrakt***

*Sve je veća zainteresovanost pravnika vezano za kompjuterski kriminal, takozvani sajber kriminal. Pošto se on sve više razvija sa razvojem inovativnosti u oblasti informacionih tehnologija, neophodne su zakonodavne mere koje će ovu vrstu kriminala regulisati i sankcionisati. Kao učestalo krivično delo, danas se pojavljuje računarska sabotaža, koja je inkriminisana krivičnim zakonodavstvom Republike Srbije. Pošto je ona Krivičnim zakonikom veoma uopšteno određena, neophodno je odrediti sam pojam računarske sabotaže, kao i njene vrste, odnosno neophodno je predstaviti neke od mnogobrojnih mogućnosti za izvršenje ovog krivičnog dela. Međunarodnopravna regulativa je od velikog značaja zbog toga što se radi o krivičnom delu gde učinioci mogu biti iz različitih zemalja i tako udruženo delovati. Međunarodna Konvencija o visokotehnološkom kriminalu je definisala pojmove koji su od značaja za određivanje pojma računarske sabotaže. Svakako, računarska sabotaža i ostala krivična dela sajber kriminala se međusobno prožimaju, te je potrebno dovesti ih u vezu, uporediti sličnosti i razlike i analizirati u kom odnosu stoje. Od naročitog značaja je razgraničiti računarsku sabotažu i sajber terorizam koji predstavlja jednu od većih opasnosti u svetu računara, računarskih mreža, interneta i društvenih mreža. S obzirom na to da je danas nemoguće funkcionisati ni za pojedinca ni za državu bez upotrebe računara i savremenih tehnologija, važna je činjenica da je sve razvijenija svest o opasnosti istih, te je stoga neophodno da države preduzmu značajne korake ka regulisanju računarske sabotaže i ostalih opasnih radnji koje se vrše putem računarske tehnologije.*

***Ključne reči:*** *računarska sabotaža, visokotehnološki kriminal, zloupotreba računara, zaštita računara, zaštita u računarskim mrežama*

***Abstract***

*There is a growing interest among lawyers in computer crime, otherwise known as cyber-crime. Since it is increasingly developing together with the development of innovations in the field of information technologies, legislative measures are necessary to regulate and sanction this type of crime. Nowadays, computer sabotage appears as a frequent criminal offense, which is incriminated by the Criminal Legislation of the Republic of Serbia. Since it is very generally defined by the Criminal Code, it is necessary to determine the very notion of computer sabotage as well as its types, i.e. it is necessary to present some of the many possibilities for the execution of this crime. International legal*

*Adresa autora*
***Živanka Miladinović Bogavac***
*zivankamiladinovic@gmail.com*

*regulation is of great importance because the criminal offense in question is the one where the perpetrators may be from different countries and thus work together. The International Convention on Cyber Crime defined terms that are important for determining the concept of computer sabotage. Certainly, computer sabotage and other criminal acts of cybercrime are mutually intertwined, and it is necessary to connect them, compare the similarities and differences and analyze in what relation they stand to each other. It is of particular importance to distinguish computer sabotage from cyber terrorism, which is one of the biggest dangers in the world of computers, computer networks, the internet, and social networks. Given that nowadays it is impossible for an individual or a country to function without the use of computers and modern technologies, it is important that the awareness about the danger of those above-mentioned spreads, and it is, therefore, necessary that countries take significant steps towards regulating computer sabotage and other dangerous activities that are carried out through computer technology.*

**Keywords:** *computer sabotage, cyber crime, computer misuse, computer protection, computer network defense*

## 1 POJAM I TEORIJSKO ODREĐENJE RAČUNARSKE SABOTAŽE

Kako bi odredili pojam i teorijsko određenje računarske sabotaže, prvo treba da je kategorizujemo pod koju vrstu kriminaliteta ona potpada. Radi se, dakle, o kompjuterskom kriminalitetu, odnosno kako je pravilnije reći u našem jeziku, o računarskom kriminalitetu. Krivična dela u okviru ove vrste su takozvana kompjuterska krivična dela, tj. dela koja su usmerena protiv bezbednosti podataka u savremenim informatičkim sistemima. Pod kompjuterskim kriminalom obično se podrazumeva kriminalitet koji angažuje kompjuter kao sredstvoili kao cilj izvršenja krivičnih dela. (Lilić & Prlja, 2008, str. 85)

U literaturi je prisutno mišljenje da kriminal u vezi s kompjuterima nije samo još jedan oblik običnog kriminala, već je to opšti vid svih oblika kriminala. U krajnjoj liniji ovaj oblik će postati dominantna varijanta, tako da će kako nenasilni, tako i nasilni kriminal biti vezan za kompjutere. Iz tih razloga, ubuduće neće biti korisno razdvajati nekompjuterski od kompjuterskog kriminala“. (Parker, 1981, str. 10)

Ukoliko u obzir uzmemo podelu kompjuterskog kriminala prema načinu izvršenja na kopjuterski kriminal izvršen putem socijalnog inžinjeringa, malicioznim programima ili kombinovanom metodom, možemo zaključiti da računarska sabotaža podpada pod 2 i 3 vrstu kompjuterskog kriminala. (Miladinović Bogavac, Models of commiting cyber criminal offences, 2018)

Računarska sabotaža kao jedno od kompjuterskih krivičnih dela, već iz naziva upućuje šta ona predstavlja u kriminalnom svetu. Reč „sabotaža“ znači namerno, ilegalno izvedeno kvarenje ili uništavanje dobara radi nanošenja štete i izazivanja haosa. (Jezikoslovac, 2018) Reč vodi poreklo iz francuskog jezika –,,*sabotage*”,što u bukvalnom smislu znači „pravljenje drvenih cipela“ (Vokabular, 2006), aludirajućina to da su u revolucionarnoj Skupštini zastupnici sabotirali govore lupajući cipelama. (Jezikoslovac, 2018)

Na osnovu člana 299 Krivičnog zakonika Republike Srbije (2014, str. član 299), možemo zaključiti da je računarska sabotaža u našem pravu određena kao unošenje, uništenje, brisanje, izmena, oštećenje, prikrivanje ili na drugi način činjenje neupotrebljivim računarskog podatka ili programa ili uništenje ili oštećenje računara ili drugog uređaja za elektronsku obradu i prenos podataka sa namerom da se onemogući ili znatno omete postupak elektronske obrade i prenosa podataka koji su od značaja za državne organe, javne službe, ustanove, preduzeća ili druge subjekte.

Kada dovedemo u vezu zakonski opis ovog krivičnog dela i etimologiju reči „sabotaža“, dolazimo do zaključka da računarska sabotaža znači upravo namerno ilegalno kvarenje ili uništavanje računara ili onoga što je u vezi sa tim (računarski podatak, program i drugi uređaj za elektronsku obradu i prenos podataka), radi nanošenja neke štete zakonom navedenim subjektima.

Kao primer ovog krivičnog dela možemo uzeti slučaj iz 2007. godine kada je radnik na svemirskom programu američke svemirske

agencije NASA namerno oštetio računar koji je trebalo da bude isporučen na međunarodnu svemirsku stanicu šatlom Endevor, tako što je presekao žice unutar kompjutera koji je trebalo da bude dostavljen. (Gerstenmajer, 2007)

Za krivično delo računarske sabotaže značajan je subjektivni element postojanja namere da se onemogući ili znatno omete postupak elektronske obrade i prenosa podataka koji su od značaja za subjekte navedene u zakonskom opisu krivičnog dela. Dakle, delo se može učiniti samo uz postojanje direktnog umišljaja, s obzirom na postojanje namere. Delo je dovršeno preduzimanjem radnje izvršenja, a objekt radnje su računarski podatak ili program.

U zakonskom tekstu mogu se uočiti dva oblika izvršenja ovog krivičnog dela:

1. unošenje, uništenje, brisanje, izmena, oštećenje, prikrivanje ili na drugi način činjenje neupotrebljivim računarskog podatka ili programa.
2. uništenje ili oštećenje računara ili drugog uređaja za elektronsku obradu i prenos podataka.

Prvi oblik ovog krivičnog dela je usmeren na računarski podatak ili program.

Prema Zakonu o izmenama i dopunama Krivičnog zakonika, računarski podatak je svako predstavljanje činjenica, informacija ili koncepta u obliku koji je podesan za njihovu obradu u računarskom sistemu, uključujući i odgovarajući program na osnovu koga računarski program obavlja svoju funkciju. Krivični zakonik definiše šta je to računarski program. Njime se smatra uređeni skup naredbi koje služe za upravljanje radom računara, kao i za rešavanje određenog zadatka pomoću računara. Kod prvog oblika krivičnog dela računarske sabotaže radnja izvršenja je postavljena alternativno. Ona može da se sastoji u uništenju, brisanju, izmeni, oštećenju ili prikrivanju računarskog podatka ili programa. (Zakon o izmenama i dopunama Krivičnog zakonika, 2009)

Drugi oblik računarske sabotaže kao objekat ima računar ili drugi uređaj za elektronsku obradu i prenos podataka.

Radnja izvršenja kod drugog oblika je takođe postavljena alternativno i može se sastojati u uništenju ili oštećenju računara ili drugog uređaja za elektronsku obradu i prenos podataka sa namerom da se onemogući ili znatno omete postupak elektronske obrade i prenosa podataka koji su od značaja za državne organe, javne službe, ustanove preduzeća ili druge subjekte.Pod uništenjem računara ili drugog uređaja za elektronsku obradu i prenos podataka treba razumeti potpuno menjanje njihovih svojstava u negativnom smislu, tako da oni faktički više i ne postoje, a pod oštećenjem takvo menjanje njihovih svojstava u negativnom smislu koje umanjuje mogućnosti njihove dalje upotrebe u svrhu kojoj su namenjeni. (Stojanović & Perić, 2009, str. 253-254)

Drugi oblik dela je dovršen takođe preduzimanjem radnje izvršenja, uz postojanje navedene namere koja u ovom slučaju i ne mora biti realizovana. S obzirom na nameru, delo se može izvršiti samo sa direktnim umišljajem. Objekt radnje predstavljaju računar ili drugi računarski uređaj za elektronsku obradu podataka. Prema Zakonu o izmenama i dopunama Krivičnog zakonika, računar je svaki elektronski uređaj koji na osnovu programa automatski obrađuje i razmenjuje podatke. (2009, str. član 25)

Kao sredstvo izvršenja dela računarske sabotaže se koriste štetni softveri ”malware“ koji se mogu klasifikovati na:

- viruse
- tzv. „trojanski konj”
- crve
- bombe i dropere
- veb – preotimanje
- steganografiju. (Vestbi, 2004, str. 46-47)

Zlonamerni programi se mogu klasifikovati i po kriterijumu samostalnosti tj. potrebe za programom u kom će maliciozan program biti sakriven na:

1. one kojima je neophodan nosilac, tj. program u koji će biti sakriveni (trojanski konj, virusi); i
2. samostalne, kojima nije neophodan nosilac, koji nezavisno deluju (crvi) (Miladinović Bogavac, 2017)

## 2 PRAVNA REGULATIVA RAČUNARSKE SABOTAŽE

Pravnu regulativu visokotehnološkog kriminaliteta, i u tom smislu i računarske sabotaže možemo gledati kroz međunarodnopravne propise i kroz propise domaćeg zakonodavstva. Treba imati na

umu da je domaće zakonodavstvo usklađeno uvek sa međunarodim načelima, jer ratifikacijom međunarodnih konvencija, Republika Srbija se obavezuje da određene oblike, u ovom slučaju pojavne oblike visokotehnološkog kriminaliteta, inkriminiše u svom pozitivnom zakonodavstvu.

23. novembra 2001. godine Savet Evrope je doneo Konvenciju o visokotehnološkom kriminalu (takozvana Konvencija o sajber kriminalitetu) u Budimpešti u originalu na engleskom i francuskom jeziku. Ubrzo, naša zemlja je posebnim zakonom potvrdila ovu Konvenciju. U preambuli Konvencije (Skupština Srbije, 2009) se ukazuje na neophodnost međunarodne saradnje u ovoj oblasti krivičnog prava „s obzirom na duboke promene koje je donela digitalizacija, konvergencija i stalna globalizacija računarskih mreža“. Takođe, ističe se da su zemlje potpisnice zabrinute zbog rizika da se računarske mreže i elektronske informacije mogu koristiti i za izvršenje krivičnih dela i da dokazi koji se odnose na takva dela mogu biti sačuvani i preneseni preko tih mreža.

Ovom konvencijom su definisani pojmovi poput računarskog sistema, računarskog podatka, davaoca usluge, podatka o saobraćaju.

Drugi deo Konvencije koji se odnosi na procesne odredbe sadrži odeljak 2 (Skupština Srbije, 2009, str. član 16, stavovi 1-2) koji je posvećen isključivo hitnoj zaštiti sačuvanih računarskih podataka, koja nalazi primenu i u slučajevima računarske sabotaže. Svaka strana ugovornica treba da usvoji zakonodavne i druge mere, neophodne da bi svoje nadležne organe ovlastila da mogu da narede ili na sličan način postignu hitnu zaštitu određenih računarskih podataka, uključujući tu i podatke o saobraćaju koji su sačuvani preko računarskog sistema, a posebno u slučaju kada ima osnova da se veruje da su podaci naročio podložni gubitku ili izmeni. Nalaže se strani ugovornici da usvoji zakonodavne i druge mere neophodne da se to lice obaveže da štiti i sačuva celovitost tih računarskih podataka za neophodan vremenski period, a najviše do 90 dana, kako bi se nadležnim organima omogućilo da zahtevaju njihovo razotkrivanje .

Računarska sabotaža, samim tim što se vrši preko računara, korišćenjem interneta ili na neki drugi način, ima elemente međunrodnog krivičnog dela, jer učinilac ili grupa učinilaca mogu imati boravište ili prebivalište u različitim državama, pri čemu s obzirom na nadležnosti svake države, može biti komplikovano doći do potencijalnih izvršilaca krivičnog dela. Zato je međunarodna saradnja od velikog značaja kod ovog dela, pa i kod ostalih sajber krivičnih dela. Konvencijom se predviđa da strane ugovornice međusobno sarađuju u najširem mogućem obimu, kroz primenu odgovarajućih međunarodnih instrumenata o međunarodnoj saradnji u krivičnim stvarima, dogovora usaglašenih na osnovu jednoobraznih ili recipročnih propisa, u svrhu istraga ili postupaka koji se odnose na krivična dela u vezi sa računarskim sistemima i podacima ili u svrhu prikupljanja dokaza u elektronskom obliku o krivičnom delu. (Skupština Srbije, 2009, str. član 23)

Računarska sabotaža je u srpskom zakonodavstvu inkriminisana u Krivičnom zakoniku RS, kao krivično delo protiv bezbednosti računarskih podataka i to u članu 299.Kako zaključujuStojanović-Perić, ovim krivičnim delom se pruža zaštita elektronskim sistemima i mrežama za elektronsku obradu i prenos podataka koji imaju poseban društveni značaj. (Stojanović & Perić, 2009, str. 253) Taj društveni značaj je upravo ono što se može postaviti kao specifičnost ovog dela u odnosu na druga kompjuterska krivična dela. Računarska sabotaža se vrši u cilju da se onemogući ili znatnoomete postupak elektronske obrade i prenosa podataka koji su od značaja za državne organe, javne službe, ustanove, preduzeća ili druge subjekte.

Predviđena sankcija za ovo krivično delo je kazna zatvora od šest meseci do pet godina.

Zakonodavac je odredio osnovni oblik ovog krivičnog dela, izostavljajući njegove privilegujuće ili kvalifikovane oblike.

## 3 ODNOS RAČUNARSKE SABOTAŽE I DRUGIH KRIVIČNIH DELA SAJBER KRIMINALA

Zajedničko za sva krivična dela sajber kriminala je to što se računar koristi kao sredstvo izvršenja krivičnog dela. Samo vršenje krivičnih dela podrazumeva upotrebu kompjutera, odnosno kompjuterskog sistema u smislu sredstva ili cilja izvršenja krivičnog dela. (Stojanović & Perić, 2009, str. 248)

Grupni zaštitni objekt ovih krivičnih dela je bezbednost računarskih podataka i računarskih mreža. Iako naš Krivični zakonik propisuje samo nekoliko krivičnih dela ove kategorije, krivičnopravna zaštita računarskih podataka i računarskih mreža je sveobuhvatnija, jer se postiže primenom inkriminacija drugih krivičnih dela koja su po pretežnijem grupnom zaštitnom objektu svrstana u druge glave (protiv imovine, protiv sloboda i prava građana, protiv industrijske svojine, protiv privrede...). (Stojanović & Perić, 2009, str. 248)

Zajednička posledica krivičnih dela sajber kriminala bi bila pričinjavanje materijalne štete po neko pravno ili fizičko lice. Za kvalifikovane oblike je karakteristično da kvalifikatornu okolnost predstavlja uvek prouzrokovanje štete preko određenog novčanog iznosa ili nastupanje štetnih posledica.

Kao oblik krivice je uvek predviđen umišljaj, s obzirom na postojanje namere kao subjektivnog obeležja. Za ova krivična dela je naročito interesantno da zakonodavac propisuje da izvršilac može biti svako lice, te se radi odelicta communia.

Član 298. Krivičnog zakonika Republike Srbije, propisuje krivično delo oštećenje računarskih podataka i programa. S obzirom na uporednu analizu računarske sabotaže i oštećenja računarskih podataka i programa, oba dela imaju zajedničke karakteristike koje se ogledaju u načinu izvršenja, a to je brisanj e, izmena, oštećenje, prikrivanje ili na drugi način činjenje neupotrebljivim računarskog podatka ili programa.

Radnja izvršenja kod ovih krivičnih dela je ista, razlike možemo primetiti u odnosu na svojstvo izvršioca, objekat krivičnog dela i zaprećenoj kazni.

U slučaju krivičnog dela oštećenje računarskih podataka i programa radi se o „neovlašćenom“ (bez odgovarajuće dozvole) preduzimanju navedenih radnji, te potencijalni izvršilac je ograničen na lica koja imaju neko ovlašćenje, dok kod računarske sabotaže to nije slučaj. U slučaju računarske sabotaže zahteva se postojanje određene namere koja je usmerena prema državnim organima, javnoj službi, ustanovi, preduzeću ili drugom subjektu, dakle onimsubjektimakoji imaju poseban društveni značaj. Radnja izvršenja krivičnog dela računarske sabotaže se preduzima sa namerom da se onemogući ili znatno omete postupak elektronske obrade i prenosa podataka koji su od značaja zadržavne organe, javnu službu, ustanove, preduzeća ili drugog subjekta.Kod oštećenja računarskog podataka i programa ova specifična namera ne postoji.Kvalifikovani oblicidela podrazumevaju da je nastupila šteta koja prelazi određeni iznos, dok kod računarske sabotaže nije određen iznos prouzrokovane štete, jer je kod nje u prvom planu postojanje namere. Sankcija predviđena za krivično delo oštećenja računarskih podataka i programa je za osnovni oblik novčana kazna ili kazna zatvora do jedne godine. U slučaju težih oblika oštećenja računarskih podataka i programa, ako je prouzrokovana šteta u iznosu koji prelazi četristopedeset hiljada dinara, učinilac će se kazniti zatvorom od tri meseca do tri godine. U najtežem slučaju ovog krivičnog dela tj. ako je prouzrokovana šteta u iznosu koja prelazi milion i petsto hiljada dinara, učinilac će se kazniti zatvorom od tri meseca do pet godina. Za krivično delo računarska sabotaža zakonodavac je predvideo kaznu zatvora od šest meseci do pet godina. (Skupština Srbije, Krivični zakonik RS, 2014, str. član 298)

Pravljenje i unošenje računarskih virusa , krivično delo predviđeno članom 300 Krivičnog zakonika Republike Srbije (2014), se sastoji u pravljenju računarskog virusa u nameri njegovog unošenja u tuđ računar ili računarsku mrežu. Radnja izvršenja podrazumeva primenu određenih tehnoloških postupaka kojima se računarski virus stvara. (Stojanović & Perić, 2009, str. 254) Upoređujući ovo delo sa računarskom sabotažom, površnom analizom mogli bismo reći da bi ovo delo moglo da se podvede pod računarsku sabotažu, samim tim što smo govorili o vidovima računarske sabotaže gde su kompjuterski virusi sredstvo da se sabotaža izvrši, dakle da se onemogući ili znatno omete postupak elektronske obrade i prenosa podataka. No, element namere koja je upravljena protiv društveno značajnih subjekata je ono što odvaja računarsku sabotažu kao zasebno krivično delo, kao i to da je delo iz člana 300. Krivičnog zakonika dovršeno samim pravljenjem računarskog virusa. Izvršilac može biti bilo koje lice, ali se ona svode na lica koja raspolažu stručnim znanjem za pravljenje računarskih virusa, tzv.virus makers.

Računarska prevara je posebno krivično delo u članu 301 Krivičnog zakonika Republike Srbije, koje ima osnovni, dva teža oblika ( s obzirom na kvalifikatornu okolnost da je delom pribavljena imovinska korist preko određenih iznosa) i lakši oblik. Osnovni oblik se sastoji u unošenju netačnog podatka, propuštanja unošenja tačnog podatka ili na drugi način prikrivanje ili lažno prikazivanje podatka i time uticanje na rezultat elektronske obrade i prenosa podataka u nameri da sebi ili drugom bude pribavljena protivpravna imovinska korist i time drugome prouzrokuje imovinska šteta. (Krivični zakonik RS, član 301) U odnosu na delo računarske sabotaže, osnovna razlika je u samoj nameri, kao i u prethodnom slučaju. U slučaju prevare, namera se sastoji u pribavljanju protivpravne imovinske koristi, dok je kod sabotaže ta namera usmerena na to dase onemogući ili znatno omete postupak elektronske obrade i prenosa podataka.

Krivična dela - neovlašćeni pristup zaštićenom računaru, računarskoj mreži i elektronskoj obradi podataka (Krivični zakonik RS, član 302) i sprečavanje i ograničavanje pristupa javnoj računarskoj mreži (Krivični zakonik RS, član 303) takođe nemaju element namere karakterističan za sabotažu. Ipak sredstvo izvršenja je isto (računar) kao i objekt radnje (računarski podatak i javna računarska mreža).

Krivično zakonodavstvo Republike Srbije predviđa još dva krivična dela protiv bezbednosti računarskih podataka – neovlašćeno korišćenje računara ili računarske mreže i pribavljanje, nabavljanje i davanje drugom sredstava za izvršenje krivičnih dela protiv bezbednosti računarskih podataka. (Krivični zakonik RS, član 304) U prvom slučaju namera je pribavljanje protivpravne imovinske koristi, što opet nije u skladu sa namerom kao kod krivičnog dela računarske sabotaže. U drugom slučaju radi se o radnji saučesništva, koja je inkriminisana kao zasebno krivično delo, te ovo delo može prethoditi izvršenju krivičnog dela računarske sabotaže.

Analizirajući odnos računarske sabotaže sa ostalim krivičnim delima sajber kriminala, ne možemo se ne osvrnuti na sajber terorizam. Sajber napadi predstavljaju novu pretnju za države i njihovu bezbednost. Terorističke organizacije manipulišući društvenim mrežama,koriste društvene mreže poput Twitter-a, Facebook-a, YouTube-a i drugih, i internet komunikaciju kao efikasno sredstvo za distribuciju svoje propagande, ideologije i slanje političkih poruka. Tri su bitna indikatora za kvalifikaciju sajberterorizma (Jonev, 2016, str. 208):

1. aktivnost mora imati političku, ideološku, religioznu, sociološku pozadinu;
2. sredstvo putem kojih se napad izvršava je kompjuter i računarske mreže;
3. napad mora imati posledicu – kao indikatori to mogu biti uništavanje informacionih sistema, fizičko uništenje objekata, ugrožavanje života civila (povreda, smrt). (Jonev, 2016, str. 210-211)

Dakle, biće krivičnog dela računarske sabotaže, ima zajedničku 2. i 3. Karakteristiku sa sajber terorizmom. Sredstvo izvršenja je isto, a to je računar, dok posledica nije ista u potpunosti. Sajber terorizam može imati za posledicu i ugrožavanje života civila, što ga kvalifikuje znatno težim krivičnim delom, a posebno kad na to dodamo i političku pozadinu koja kod računarske sabotaže ne postoji.

## 4 ZAKLJUČAK

S obzirom da je svakodnevni život vezan za računare, da se sprovodi digitalizacija u svim društvenim oblastima i društvenim institucijama, neophodno je zaštititi sistem od sajber kriminala i računarskih sabotaža koje su neizbežne, jer su računari dostupni svima, te i onima koji žele da ih koriste kao sredstvo izvršenja krivičnog dela. Računarska sabotaža je sve češća, jer se učinioci teško otkrivaju, a poznavaocima informacionih tehnologija koji se odluče za kriminal, s obzirom na njihova stručna znanja u ovoj oblasti, nije preveliki problem da se u tako nešto upuste samim tim što su svesni da za njihovo otkrivanje takođe treba posedovati visoke kvalifikacije. Međutim, s obzirom na to da je mnogo veći broj izvršenja ovog krivičnog dela kao i posledica koje su njime prouzrokovane, u odnosu na broj kompetentnih stručnjaka u ovoj oblasti kriminologije, svakako treba raditi na edukaciji onih koji se bave sajber kriminalom. Razvoj digitalne forenzike je od naročitog značaja, jer ona predstavlja noviji način u istrazi krivičnog dela. U smislu pravne regulative, Republika Srbija je dosta napredovala inkriminišući određen broj krivičnih dela protiv bezbednosti računarskih podataka. Možemo

primetiti da kao i u svim oblicima kriminaliteta, značajna je prevencija, a nakon toga kaznena politika. Možemo smatrati da kaznena politika naše zemlje polako dostiže nivo kaznenih politika ostalih evropskih zemalja. Takođe, Zakonom o potvrđivanju Konvencije o visokotehnološkom kriminalu, zagarantovana je međunarodna saradnja strana ugovornica koja je neophodna kada se radi o računarskoj sabotaži. Akcenat treba staviti na prevenciju koja bi trebalo da se razvija u smeru izrađivanja i ugrađivanja u računarske softvere programa (najčešće bi to bili antivirus programi) koji neće dozvoliti da do sabotaže uopšte dođe. Što su značajniji podaci koji se čuvaju u bazi informacionog sistema, to bi softverska zaštita od računarske sabotaže trebalo da bude veća. Zakon u oblasti prevencije treba da obezbedi, tj. propiše precizno u kojim slučajevima se daje sudska dozvola za presretanje i otkrivanje sadržaja kompjuterskih komunikacija i podataka. Ovakve odredbe bi mogle da budu suprotstavljene pravu na privatnost, te zbog toga treba istaći da bi one morale biti izuzetno precizne i formulisane tako da ne postoje pravne praznine koje bi onemogućile otkrivanje izvršilaca krivičnog dela računarske sabotaže.

## CITIRANA DELA

Gerstenmajer. (2007, 07 28). Sabotaža u NASA. *Danas*. Preuzeto sa https://www.danas.rs/zivot/sabotaza-u-nasa/

Jezikoslovac. (2018, 08 07). ***sabotaža***. Preuzeto sa Jezikoslovac: https://jezikoslovac.com/word/0zep

Jonev, K. (2016). Sajber terorizam i upotreba sajber prostora u terorističke svrhe. *Bezbednost*(2).

Lilić, S., & Prlja, D. (2008). *Pravna informatika veština – Internet za pravnike.* Beograd: Dosije.

Miladinović Bogavac, Ž. (2017). Pojam, vrste i načini delovanja malicioznih programa kojima se sprovode internet prevare. *Časopis za istraživanje medija i društva Medijski dijalozi, X*(29), 239.

Miladinović Bogavac, Ž. (2018). Models of commiting cyber criminal offences. *Međunarodna naučna konferencija ,,PRAVO 2018" Zbornik radova, Poslovni i pravni fakultet Univerzitet Union Nikola Tesla* (str. 122-129). Beograd: ICIM Izdavački centar za industrijski menadžment.

Parker, D. (1981). *Fighting Computer Crime.* New York: Charles Scribner & Sons.

Skupština Srbije. (2009). Zakon o izmenama i dopunama Krivičnog zakonika. *Sl. glasnik RS", br. 72/2009*.

Skupština Srbije. (2009). Zakon o potvrđivanju Konvencije o visokotehnološkom kriminalu. *Sl. glasnik RS – Međunarodni ugovori", br. 19/2009*.

Skupština Srbije. (2014). Krivični zakonik RS. *Sl. glasnik, br. 108/2014*.

Stojanović, Z., & Perić, O. (2009). *Krivično pravo – posebni deo.* Beograd.

Vestbi, D. (Ur.). (2004). *Međunarodni vodič za borbu protiv kompjuterskog kriminala.* Beograd: Američka advokatska komora.

Vokabular. (2006). *Sabotaža*. Preuzeto sa Vokabular: https://vokabular.org/?search=sabota%C5%BEa&lang=sr-lat