KAZNENOPRAVNA ZAŠTITA RAČUNALNIH SUSTAVA, PROGRAMA I PODATAKA

Pregledni znanstveni rad

UDK 343.7
004.3/.4

Primljeno: 8. listopada 2014.

Ivica Kokot*

Većina država u svijetu načelno se složila u potrebi da se najteži napadi na informacijske sustave kriminaliziraju, iako i na međunarodnoj i na nacionalnoj razini nailazimo na različite pristupe. Najvažniji međunarodni instrument u borbi protiv kompjutorskog kriminala, Konvencija o kibernetičkom kriminalu Vijeća Europe iz 2001. godine, s vremenom se pokazao nedostatnim, tako da su Europski parlament i Vijeće EU-a donijeli Direktivu o napadima na informacijske sustave, kojom bi manjkavosti Konvencije trebale biti otklonjene. Odredbe Konvencije i prijedloga Direktive R. Hrvatska preuzela je u novo kazneno zakonodavstvo, kao i obveze koje iz toga proizlaze. Kako se radilo o jedinstvenoj prilici da se kod donošenja novog Kaznenog zakona, koji je stupio na snagu 1. 1. 2013. godine, područje kriminalizacije prvi put sustavno uredi, ovaj rad testirat će uspješnost novih odredaba poredbenom i drugim metodama.

Ključne riječi: kibernetički kriminalitet, napadi na informacijske sustave, računalni sustavi, računalni programi, računalni podaci

1. KAZNENOPRAVNI OKVIR KRIMINALIZACIJE NAPADA NA INFORMACIJSKE SUSTAVE U REPUBLICI HRVATSKOJ

Reformom hrvatskog kaznenog zakonodavstva 1997. godine uvedeno je prvo pravo kazneno djelo računalnog kriminaliteta u članku 223. KZ-a pod nazivom „Oštećenje i uporaba tuđih podataka" u Glavi XVII. Kaznena djela protiv imovine.

U isto vrijeme, 1997. godine Vijeće Europe otišlo je korak dalje i osnovalo Odbor stručnjaka za kriminalitet u kibernetičkom prostoru, koji je radio na izradi međunarodnog instrumenta za suzbijanje kriminaliteta u kibernetičkom prostoru.[1] Razlog takvoj aktivnosti bio je nagli razvoj informacijsko-komunikacijskih tehnologija, prije svega interneta, a time i kaznenih djela na internetu, čime je kazneno pravo usmjereno na kompjutorski kriminalitet postalo preusko, pa se kaznenopravna zaštita proširila na cijeli kibernetički prostor. Konvencija o kibernetičkom kriminalitetu (ETS 185) usvojena je na

* Ivica Kokot, univ. spec. crim., polaznik poslijediplomskog doktorskog studija na Pravnom fakultetu Sveučilišta u Zagrebu

[1] *Explanatory Report to the Convenction on Cyber Crime*, II. The Preparatory Work, alineja 12., dostupno na http://conventions.coe.int/Treaty/en/Reports/Html/185.htm (7. 1. 2014.)

konferenciji Vijeća Europe u Budimpešti 23. 11. 2001. godine, gdje je otvorena za potpisivanje i tada ju je potpisala i Republika Hrvatska. Konvencija je objavljena u *NN - Međunarodni ugovori* broj 9/2002. U odnosu na Republiku Hrvatsku, Konvencija je stupila na snagu 1. 7. 2004. godine. Konvencijom su države stranke preuzele obvezu da usvoje takve zakonske i druge mjere kojima bi se omogućio kazneni progon počinitelja kaznenih djela protiv tajnosti, integriteta i dostupnosti računalnih sustava i podataka, kaznenih djela u svezi s računalom, kaznenih djela u svezi sa sadržajem, kao i kaznenih djela u vezi s povredama autorskih i drugih srodnih prava te kažnjavanje pokušaja, poticanja i pomaganja tih djela. Osim sankcioniranja, Konvencijom je predviđeno i rješavanje pojedinih procesnih pitanja.

Zakonom o izmjenama i dopunama Kaznenog zakona objavljenim 15. 7. 2004. godine u *NN* 105/2004. unesena je u kazneno zakonodavstvo novela članka 223., koji je promijenio naziv u "Povreda tajnosti, cjelovitosti i dostupnosti računalnih podataka, programa ili sustava" te su dodani članci 223. a) "Računalno krivotvorenje" i 224. a) "Računalna prijevara", koji su stupili na snagu 1. 10. 2004., čime je kazneno zakonodavstvo usklađeno s odredbama Konvencije.

Sljedeća velika kaznenopravna reforma u Republici Hrvatskoj dogodila se 2011. godine, kad je donesen novi Kazneni zakon, objavljen u *NN* br. 125/2011., koji je stupio na snagu 1. 1. 2013. godine. Novim, aktualnim Kaznenim zakonom kaznena djela protiv računalnih sustava, programa i podatka izdvojena su iz glave kaznenih djela protiv imovine u posebnu glavu XXV. pod nazivom „Kaznena djela protiv računalnih sustava, programa i podataka". Prema Obrazloženju uz Kazneni zakon[2] kaznena djela protiv računalnih sustava i programa usklađena su s Konvencijom o kibernetičkom kriminalu, a Glava XXV. obuhvaća osam kaznenih djela iz članka 266. „Neovlašteni pristup", članka 267. „Ometanje računalnog sustava", članka 268. „Oštećenje računalnih podataka", članka 269. „Neovlašteno presretanje računalnih podataka", članka 270. „Računalno krivotvorenje", članka 271. „Računalna prijevara", članka 272. „Zlouporaba naprava" i članka 273. „Teška kaznena djela protiv računalnih sustava, programa i podataka".

Nedugo nakon ulaska Republike Hrvatske u Europsku uniju 12. 8. 2013. godine Europski parlament i Vijeće Europske unije, temeljem članka 83. stavka 1. Ugovora o funkcioniranju Europske unije,[3] donijeli su Direktivu 2013/40/EU o napadima na informacijske sustave i o zamjeni Okvirne odluke Vijeća 2005/222/PUP.[4] Ciljevi su Direktive 2013/40/EU, među ostalim, približiti kaznena prava država članica u području napada na informacijske sustave utvrđivanjem minimalnih pravila o definiranju kaznenih djela i odgovarajućih sankcija. Direktiva 2013/40/EU nije u suprotnosti s Konvencijom o kibernetičkom kriminalu, nego se na nju nadovezuje. O Konvenciji se govori kao o referentnom okviru za borbu protiv kibernetičkog kriminala, uključujući i napade na informacijske sustave.

[2] *Konačni prijedlog Kaznenog zakona*, Obrazloženje, P.Z.E. br. 866, dostupno na http://www.sabor.hr/Default.aspx?art=41259 (7. 1. 2014.)
[3] Official Journal of the European Union (Službeni list Europske unije, dalje: SL), C 236, 26. 10. 2012.
[4] SL L 218, 14. 8. 2013.

Dovršetak procesa ratifikacije Konvencije od svih država članica u najkraćem mogućem roku postavlja se kao prioritet.

Razloge za donošenje Direktive uz već postojeću Konvenciju treba tražiti u naravi Konvencije, nedovoljnoj harmonizaciji kaznenog prava na području napada na informacijske sustave te manjkavostima glede sadržaja. Sam postupak izmjena i dopuna Konvencije dugotrajan je, skup i kompliciran, za razliku od postupka unutar EU-a nakon Lisabonskog ugovora. Kod harmonizacije kako materijalnog tako i procesnog prava ostavljene su brojne rezervacije država članica na odredbe Konvencije, osobito glede prekograničnog pristupa podacima.[5]

Značajnije novine uvedene Direktivom u području materijalnog prava jesu: proširenje kažnjivog ponašanja, uvođenje otežavajućih okolnosti te određivanje visine kazni.[6] Države članice u obvezi su donijeti zakone i druge propise za usklađivanje do 4. rujna 2015. godine.

2. INFORMACIJSKI SUSTAVI I KIBERNETIČKI KRIMINAL

2.1. Kriminalitet u virtualnom svijetu

Određivanju kriminala u virtualnom prostoru moguće je pristupiti na različite načine. Za potrebe ovog rada koristit ćemo definicije preuzete u Kazneni zakon RH iz Konvencije o kibernetičkom kriminalu VE[7] i Direktive 2013/40/EU jer, usprkos brojnim prigovorima, ipak se radi o rješenju oko kojeg postoji konsenzus velikog broja država relevantnih za kaznenopravnu suradnju na području informacijske sigurnosti.

U Konvenciji VE sam pojam *cybercrime* pojavljuje se na svega nekoliko mjesta. Prije svega pojavljuje se u samom naslovu *Convention on cybercrime*, u kojem je leksička osnova *cyber* prevedena na hrvatski kao „kibernetički". Iako se u načelu prilikom prijevoda polazi od korijena riječi na latinskom, grčkom ili drugom jeziku, što bi u ovom slučaju bila grčka riječ *kiber*, sam pojam kibernetički odnosi se na znanost o istraživanju i automatskim sustavima kontrole u strojeva i živih bića, istraživanje procesa upravljanja raznim sustavima (biološkim, tehničkim, ekonomskim i dr.).[8] No ako dalje pratimo pojavljivanje leksičke osnove *cyber* u Konvenciji, vidimo da se javlja u preambuli te na samom kraju u članku 46., koji se odnosi na savjetovanje stranaka. Stoga se može zaključiti da pojam *cybercrime* ima više kriminalnopolitičko značenje te da svoj sadržaj crpi iz ukupnog

[5] TC-Y Guidance note # 3, Transborder access to data (Article 32), dostupno na: http://www.coe.int/t/dghl/cooperation/economiccrime/Source/Cybercrime/TCY/TCY%202013/TCY_2013_7E_GN3_transborder_V2public.pdf (7. 1. 2014.)

[6] Explanatory Memorandum of the Proposal for directive on attacks against information system, Brussels, 30. 9. 2010., COM(2010), 517 final, str. 6-9. ,

[7] Council of Europe Convention on Cybercrime, dostupno na http://conventions.coe.int/Treaty/en/Treaties/Html/185.htm (8. 1. 2014.)

[8] Hrvatski jezični portal, dostupno na http://hjp.novi-liber.hr/index.php?show=search (9. 1. 2014.)

sadržaja Konvencije, odnosno da *cybercrime* čine sva kaznena djela koja su opisana u odjeljku 1. - kazneno materijalno pravo. Na sličan način pojam *cybercrime* koristi se i u Direktivi 2013/40/EU. Rijetki ga pravni instrumenti, bilo na međunarodnoj bilo na nacionalnoj razini, definiraju ili koriste za određivanje konkretnog sadržaja, već više kao pravnog okvira jer međunarodni instrumenti to i ne traže.

2.2. Informacijski sustav

Povijesno gledano, pravno relevantni sadržaj pojma „informacijski sustav" dolazi iz definicije koju je OECD usvojio u svojim Smjernicama za sigurnost informacijskih sustava 1992. godine.[9] Svoj konačni oblik pojam je dobio u Konvenciji VE iz 2001. godine i u Okvirnoj odluci Vijeća EU 2002. godine o napadima na informacijske sustave.[10]

Prema definiciji iz čl. 2. Konvencije računalni sustav označava svaku napravu ili skupinu međusobno spojenih ili povezanih naprava, od kojih jedna ili više njih na osnovi programa automatski obrađuje podatke. U dopunjenom obliku definicija je preuzeta u Okvirnu odluku Vijeća 2005/222/PUP, poslije Direktivu EU-a o napadima na informacijske sustave, kao i u kazneno zakonodavstvo RH. Kao takva, definicija obuhvaća i računalne podatke koji su u računalo spremljeni, obrađeni, učitani ili preneseni za svrhe njegova rada, korištenja, zaštite i održavanja.

U definiciji pojma računalni ili informacijski sustav izraz „related devices" iz Konvencije preveden je kao „povezane naprave" te se takav koristi i u Kaznenom zakonu RH, dok je isti taj izraz iz Okvirne odluke EU-a, poslije Direktive, koja je poslužila kao model definiciji računalnog sustava u Kaznenom zakonu RH, preveden drugačije, kao „srodni uređaji".[11]

Takva rješenja kod samog prijevoda i implementacije dovode do konfuzije, pa nas sama gramatička metoda tumačenja zakona ne može dovesti do sadržaja i opsega pojma. Gramatičku je metodu stoga potrebno proširiti, odnosno prije svega koristiti njezinu inačicu, poredbenu (komparativnu) metodu, ali i sve ostale metode tumačenja zakona.[12]

Obrazloženje uz Konvenciju VE ETS 185[13] precizira sadržaj pojma računalnog sustava pa se navodi da računalni sustav, osim *hardvera*, pokriva i sistemski *softver* te da je razvijen za automatsku obradu digitalnih podataka. On može uključiti ulazne i izlazne jedinice te uređaje za pohranu podataka, može stajati sam ili biti povezan u mrežu s drugim sličnim uređajima. „Automatska obrada" označava obradu bez izravne ljudske intervencije.

[9] OECD Guidelines for the Security of Information System, dostupno na: http://www.oecd.org/internet/ieconomy/oecdguidelinesforthesecurityofinformationsystems1992.htm (15. 1. 2014.)
[10] Proposal for a Council Framework Decision on attacks against information system, SL C 203 E, 27. 8. 2002.
[11] Turković, K.; Novoselec, P.; Grozdanić, V.; Kurtović Mišić, A.; Derenčinović, D.; Bojanić, I.; Munivrana Vajda, M.; Mrčela, M.; Nola, S.; Roksandić Vidička, S.; Tripalo, D.; Maršavelski, A. *Komentar Kaznenog zakona i drugi izvori novog hrvatskog kaznenog zakonodavstva,* Narodne novine, Zagreb, 2013, str. 129.
[12] Novoselec, P.; Bojanić, I. *Opći dio kaznenog prava*, Pravni fakultet Sveučilišta u Zagrebu, Zagreb, 2013, str. 84-93.
[13] *Explanatory Report to the Convention on Cyber Crime*, *op.cit.* (bilj. 1.), čl. 1 (a), Računalni sustav.

„Obrada podataka" znači da se podacima u računalnom sustavu upravlja izvršenjem računalnog programa. Nadalje, u obrazloženju Konvencije iz 2001. godine navodi se da se računalni sustav sastoji od različitih uređaja te je potrebno razlikovati procesor ili središnju procesorsku jedinicu od periferije. Periferiju čine uređaji koji izvode određenu specifičnu funkciju u interakciji s procesorskom jedinicom, kao što su printer, videoekran, CD čitač/pisač ili uređaji za pohranu podataka.

Sa strelovitim razvojem tehnologije, koja je prešla okvire središnjeg i stolnog računala, pojavila se potreba za savjetovanjem među državama članicama. Temeljem članka 46. Odbor stranaka Konvencije izdao je 2012. godine Smjernice,[14] prema kojima definicija računalnog sustava obuhvaća i moderne uređaje kao što su mobilni telefoni, pametni telefoni, PDS uređaji, tableti i sl. jer i oni imaju mogućnost proizvodnje, obrade ili prijenosa podatka, osobito jer imaju pristup internetu, omogućuju slanje elektroničke pošte, prosljeđivanje poveznica, slanje sadržaja ili skidanje dokumenata.

S daljnjim razvojem tehnologije od vremena izdavanja Smjernica Odbora pojavio se čitav niz novih uređaja, razvio se internet praktično svega, a što je još važnije, pojavljuju se novi koncepti poimanja i korištenja samog kibernetičkog prostora, stvara se novi hibridni svijet[15] kao mješavina realnog i virtualnog, koji će također biti potrebno pravno urediti i definirati.

2.2.1. Računalne mreže

Računalna mreža, prema obrazloženju iz Konvencije VE ETS 185, jest veza između jednog ili više računalnih sustava, žičana ili bežična. Mreža može biti ograničena na manje područje (*local area networks*) ili može pokrivati široko područje (*wide area networks*) i takve mreže mogu biti međusobno povezane.

Internet je globalna mreža koja se sastoji od više međusobno povezanih mreža koje sve koriste iste protokole. Druge vrste mreža postoje, neovisno o tome jesu li spojene na internet, ukoliko mogu slati podatke između računalnih sustava. Računalni sustavi mogu biti povezani na mrežu kao krajnje točke ili predstavljati sredstvo komunikacije na mreži. Ključno je da se podaci putem mreže razmjenjuju.

Direktivom 2002/21/EZ o zajedničkom regulatornom okviru za elektroničke komunikacijske mreže i usluge Europskog parlamenta i Vijeća EU-a definirana je elektronička komunikacijska mreža koja označava prijenosne sustave, prema potrebi opremu za prospajanje ili usmjeravanje i druga sredstva koja omogućavaju prijenos

[14] T-CY Guidance Note # 1 On the notion of „computer system", Article 1a, dostupno na http://www.coe.int/t/dghl/cooperation/economiccrime/Source/Cybercrime/TCY/TCY2012/T-CY%28 2012%2921E_guidanceNote1_article1_final.pdf (15. 1. 2014.)

[15] Curvelo, P.; Guimarães Pereira, A.; Boucher, P.; Breitegger, M.; Ghezzi, A.; Rizza, C.; Tallacchini, M.; Vesnic-Alujevic, V. *The constitution of the hybrid world,* Europska komisija, JRC Scientific and policy reports, Lisabon, 2014, str. 2.

signala žičanim, radijskim, svjetlosnim ili drugim elektromagnetskim sustavom, uključujući satelitske mreže, nepokretne zemaljske mreže (komutirana mreža s prospajanjem kanala i prospajanjem paketa, uključujući internet) i zemaljske mreže pokretnih komunikacija, elektroenergetske kabelske sustave u mjeri u kojoj se koriste za prijenos signala, radiodifuzijske mreže i mreže kabelske televizijske, bez obzira na vrstu podataka koje prenose.[16]

Sukladno europskoj pravnoj regulativi, u Republici Hrvatskoj elektronička mreža definirana je čl. 2., st. 1., toč. 7. Zakona o elektroničkim komunikacijama (*NN* 73/08, 90/11, 133/12, 80/13, 71/14), a slično je stanje i u zakonodavstvima drugih članica EU-a. Pojam „računalna mreža" nalazimo na nekoliko mjesta u KZ-u RH, i to u čl. 147. Uvreda, čl. 148. Sramoćenje, čl. 149. Kleveta, čl. 151. Javno objavljivanje presude za kaznena djela protiv časti i ugleda i čl. 165. Upoznavanje djece s pornografijom, u kontekstu da se sadržaj, među ostalim, „putem računalnog sustava ili mreže¨ učini pristupačnim većem broju osoba.

Način na koji je uveden pojam mreža, uz izraz računalni sustav, otvara pitanje njegova tumačenja. Dvojbeno je odnosi li se pridjev računalni i na mrežu te odvaja li se_time računalna mreža od računalnog sustava ili se pojam „mreža" tumači samostalno bez pridjeva računalna te označava i druge mreže osim računalne.

Prema dosadašnjoj pravnoj teoriji i praksi na području kriminalizacije računalnog kriminaliteta, računalne mreže razmatrale su se u okviru pojma računalnog sustava, stoga je uvođenje pojma mreže uz računalni sustav, iako zvuči efektno, zbunjujuće. U tom smislu pojam mreže može se jedino protumačiti kao svaka mreža kojom se sadržaj učini dostupnim većem broju osoba.

2.3. Računalni programi i podaci

Niti Konvencija VE ETS 185, niti Direktiva 2013/40/EU ne definiraju posebno pojam računalnog programa, nego ga opisuju kao dio pojma računalnog podatka.[17] KZ RH računalni program definira kao skup računalnih podataka koji su u stanju prouzročiti da računalni sustav izvrši određenu funkciju. Uzimajući u obzir navedeno, primjećujemo da se radi o cirkularnim definicijama koje definiraju same sebe. U Konvenciji i Direktivi računalni je podatak tako računalni program, a u KZ-u RH računalni je program računalni podatak. Posljedica je toga da uz svaki preuzeti članak iz Konvencije KZ RH uz pojam računalni podaci dodaje još i posebnu vrstu računalnih podataka, a to su računalni

[16] Direktiva 2002/21/EZ o zajedničkom regulatornom okviru za elektroničke komunikacijske mreže i usluge Europskog parlamenta i Vijeća EU-a, SL L 108, 7. 3. 2002., čl. 2a,

[17] Konvencija o kibernetičkom kriminalu, članak 1., točka b), izrazom »računalni podaci« označava svako iskazivanje činjenica, informacija ili koncepata u obliku prikladnom za obradu u računalnom sustavu, uključujući i program koji je u stanju prouzročiti da računalni sustav izvrši određenu funkciju.

programi. S obzirom na navedeno, uputno je držati se definicije pojma programa iz Konvencije ili Direktive 2013/40/EU.

Uz informacijske sustave i programe, računalni podaci treći su izraz koji se najčešće upotrebljava na području inkriminacije napada na računalne sustave. Prema Konvenciji ETS 185, Direktivi 2013/40/EU i KZ-u RH, računalni podaci označavaju svako predstavljanje činjenica, informacija i zamisli u obliku prikladnom za obradu u informacijskom sustavu, a prema Direktivi i Konvenciji uključuju još i odgovarajući program kojim informacijski sustav provodi određenu funkciju.

Prema obrazloženju Prijedloga Okvirne odluke Vijeća Europske Zajednice iz 2002. godine o napadima na informacijske sustave, izraz računalni podatak izrađen je po uzoru na definiciju koju je stvorila Međunarodna organizacija za standardizaciju (ISO). Izraz ne bi trebao uključivati materijalne predmete, međutim, uključuje primjerice knjigu pohranjenu u obliku računalnog podatka ili pretvorenu u računalni podatak skeniranjem. Iz tog razloga definicija jasno navodi da računalni podaci trebaju biti izrađeni ili stavljeni u oblik prikladan za obradu u informacijskom sustavu ili oblik koji je prikladan izazvati neku funkciju računalnog sustava.[18]

2.4. Informacijski sustavi i podaci na globalnoj razini

Učinkovita prevencija i borba protiv kibernetičkog kriminaliteta ne može se provoditi izolirano na nacionalnoj razini jer kibernetički kriminalitet ne poznaje prostorna ograničenja. Učinkovita prevencija i borba provodi se na međunarodnoj, regionalnoj ili globalnoj razini.

Ranije definirane pojmove stoga je potrebno razmotriti i izvan okvira nacionalnog, odnosno regionalnog okvira. Osim Konvencije VE i Direktive EU-a, u ovom će se radu uzeti u obzir i pravne definicije pojmova međunarodnih instrumenata donesenih unutar Zajednice neovisnih država (CIS), Šangajske organizacije za suradnju (SCO), međuvladinih organizacija Afrike, Lige arapskih država, Ujedinjenih naroda i sličnih. Broj definicija pojmova unutar pravnih instrumenata kreće se od svega nekoliko, kao što je to slučaj kod Konvencije VE ETS 185 i Direktive 2013/40/EU, pa do dvadesetak definicija.

Govoreći o osnovnim pojmovima, neki međunarodni instrumenti i ne definiraju računalni sustav, kao, primjerice, Sporazum o suradnji država članica Zajednice neovisnih država u borbi protiv djela povezanih s računalnim podatkom ili Sporazum o suradnji u polju međunarodne informacijske sigurnosti Šangajske organizacije za suradnju. Neki za isti sadržaj umjesto pojma računalni sustavi koriste i izraze informacijski sustav ili kompjutorski sustav.

[18] *Explanatory Report to the Convention on Cyber Crime*, *op. cit.* (bilj. 1.), alineja 25.

Većina međunarodnih instrumenata koristi istu osnovu za definiranje računalnog sustava, a isto tako i podatka i mreže. Razlikuju se najčešće u naglašavanju pojedinih elemenata koji nisu isključeni iz definicija drugih instrumenata, odnosno najčešće su i sadržani u predgovoru, uvodu, obrazloženju i tumačenju. Tako se za informacijski sustav, primjerice, propisuje i da uređaj ili više njih budu sposobni obraditi podatke automatski, velikom brzinom ili prema programu.

Drugi pristupi definiciju sustava vežu uz uređaje za pohranu, obradu ili promet podataka. Definicija informacijskog sustava u modelu zakonskog teksta ITU/CARICOM/CTU o kibernetičkom kriminalu posebno spominje i internet.

Pojmovi informacijskog sustava, programa i podatka definirani u međunarodnim instrumentima čine dostatnu osnovu za ostvarivanje suradnje u borbi protiv kibernetičkog kriminala.

3. TIPOLOGIJA KAZNENIH DJELA NAPADA NA INFORMACIJSKE SUSTAVE

Pojmovi informacijski sustav, programi i podaci osnova su za određivanje opsega zaštićenog pravnog dobra. Kod kibernetičkih kaznenih djela u užem smislu štiti se njihova povjerljivost, cjelovitost i raspoloživost. Povjerljivost osigurava da informacijski sustavi, programi i podaci budu dostupni samo za to ovlaštenim korisnicima. Cjelovitost osigurava informacijske sustave, programe i podatke od neovlaštenih izmjena. Raspoloživost osigurava da informacijski sustavi, podaci i programi budu uvijek dostupni ovlaštenim korisnicima. Kod kibernetičkih kaznenih djela u širem smislu informacijski sustavi, programi i podaci štite se od raznih oblika zlouporaba. U tim slučajevima dolazi do konkurencije više pravnih dobara. Ovisno o ocjeni prevladavajućeg pravnog dobra, takve inkriminacije različito se raspoređuju unutar odredaba kaznenog zakona.

Informacijski sustavi, programi i podaci tako se mogu štititi kaznenopravnim odredbama kojima se štite druga pravna dobra, primjerice imovina, privatnost, opća sigurnost i sl. te ne postoje odredbe koje bi se primjenjivale samo na to područje. Potom je moguće da postoje specijalne odredbe koje se odnose na dio ili na sva kaznena djela kibernetičkog kriminaliteta. U slučaju da postoje posebne odredbe o kibernetičkom kriminalu, moguće je da su one sadržane u glavnom ili u posebnom, sporednom kaznenom zakonu. Daljnja je sistematizacija moguća prema kriterijima opsega materije koja se uređuje posebnim odredbama.

3.1. Kaznena djela protiv tajnosti, cjelovitosti i dostupnosti računalnih podataka i sustava

3.1.1. Neovlašteni pristup

Kaznenim djelom neovlaštenog pristupa, tzv. *hackingom*, kriminalizira se nezakoniti pristup tuđem računalnom sustavu. *Hacking* postoji od postanka informacijskog sustava. Kriminalizacijom neovlaštenog pristupa štiti se prije svega integritet računalnog sustava. Neovlašteni pristup računalnom sustavu može se figurativno usporediti s povredom nepovredivosti doma. Pravno dobro stoga nije povrijeđeno samo kad osoba bez ovlaštenja zamijeni ili „ukrade podatke" koji se nalaze u informacijskom sustavu nego i kada ga samo razgledava. Neovlašteni pristup sustavu u osnovnom obliku ne zahtijeva ni da počinitelj zaista pristupi datotekama ili pohranjenim podacima kao krajnjem cilju. Sam pristup nije posebno definiran, stoga je kao pojam otvoren i za daljnji razvoj, a obuhvaća i pristup internetom, bežičnim komunikacijskim sredstvom, kao i neovlašten pristup računalu koje nije spojeno ni na jednu mrežu. Pristup sustavu putem otvorene javne veze nije neovlašten, kao niti pristup po ovlaštenju vlasnika ili korisnika sustava. Međutim, činjenica da je žrtva kaznenog djela predala lozinku ili pristupni kod počinitelju ne znači nužno i da je počinitelj ovlašteno pristupio sustavu. Ako je počinitelj uvjerio žrtvu da mu otkrije lozinku, primjerice putem socijalnog inženjeringa, potrebno je provjeriti pokriva li to ovlaštenje i poduzetu radnju.

Motivi i ciljevi napada različiti su. Kad je u pitanju motivacija, neki počinitelji ograničavaju svoje napade na zaobilaženje sigurnosnih mjera radi dokazivanja sposobnosti, neki drugi politički su motivirani, no većina ih predstavlja samo pripremnu radnju za počinjenje drugih, težih kaznenih djela i predstavljaju nužni prvi korak.[19] U tom je slučaju stjecaj ovog i težeg kaznenog djela samo prividan jer teže djelo konzumira pripremnu radnju.

Većina država propisuje neovlašteni pristup računalnom sustavu kao posebno kazneno djelo. Manji broj država neovlašteni pristup pokriva općim odredbama, dok nekoliko država u svijetu uopće ne kriminalizira neovlašteni pristup.

Zaštitni objekt kod kaznenih djela neovlaštenog pristupa jest računalni sustav, bilo cijeli bilo neki njegov dio. No moguće je da se zaštitni objekt iz kriminalnopolitičkih razloga ograniči na računalne podatke ili informacije ili da se kriminalizira oboje u istom ili različitim člancima. Objekt zaštite može se suziti još i više time da se ograniči na određenu vrstu informacija, primjerice na one koje su zaštićene zakonom, kao što je to propisano u

[19] Understanding Cybercrime: Phenomena, Challenges and Legal Response, ITU 2012, dostupno na: http://www.itu.int/en/ITU-D/Cybersecurity/Documents/CybcrimeE.pdf (30. 9. 2014.) str. 17-18.

Sporazumu o suradnji između država članica Saveza nezavisnih država u suzbijanju kaznenih djela povezanih s računalnim informacijama (sporazum CIS-a).[20]

Daljnje razlikovanje moguće je s obzirom na to kriminalizira li se sam neovlašteni pristup ili se traži daljnja namjera ili radnja. Tako, primjerice, Konvencija VE ostavlja državama članicama mogućnost propisivanja da kazneno djelo neovlaštenog pristupa bude počinjeno povredom sigurnosnih mjera s namjerom pribavljanja računalnih podataka ili s drugom nepoštenom namjerom ili u pogledu računalnog sustava koji je spojen s drugim računalnim sustavom. Direktiva EU-a o napadima na informacijske sustave propisuje da države članice poduzimaju potrebne mjere kojima se osigurava da se bespravni pristup kažnjava kao kazneno djelo ako je počinjen kršenjem sigurnosne mjere, barem kad nije riječ o lakšim slučajevima. Sporazumom CIS-a propisano je da se neovlašteni pristup kažnjava ako takav postupak rezultira uništenjem, blokiranjem, mijenjanjem ili kopiranjem podataka ili narušavanjem funkcioniranja računala, računalnog sustava ili povezanih mreža.

Dodatni zahtjevi, osobito za poduzimanje daljnjih radnja, mogu dovesti do problema u razlikovanju tog kaznenog djela od kaznenih djela ometanja rada računalnog sustava, oštećenja računalnih podataka ili neovlaštenog presretanja računalnih podataka. Moguće je i takvo pravno tehničko rješenje gdje je neovlašteni pristup samo jedan od elemenata kaznenog djela ometanja rada računalnog sustava. Kazneno djelo ometanja rada računalnog sustava postojat će samo ako je počinjeno neovlaštenim pristupom kao nužnim prvim korakom.

Svi ranije spomenuti međunarodni instrumenti zahtijevaju da je neovlašteni pristup počinjen s namjerom. Nacrt Konvencije Afričke unije[21] te Nacrt Direktive ECOWAS[22] zahtijevaju da je neovlašteni pristup ostvaren prijevarom.

Oblici mentalnog elementa u kaznenim djelima na razini država jesu namjera, znanje, htijenje i prijevarna namjera. Međutim, moguće je naći i rješenja u kojima je dovoljna i nesmotrenost počinitelja, odnosno nehajni oblik krivnje. Nekoliko međunarodnih instrumenata predviđa i otežavajuće okolnosti. Za ovaj rad najvažnije su odredbe Direktive 2013/40/EU, koja u čl. 9. propisuje kaznene okvire.

Konvencija VE ETS 185 ne navodi posebno otežavajuće okolnosti, već samo čl. 13., koji se odnosi na sankcije i mjere te nalaže usvajanje zakonskih i drugih mjera potrebnih kako bi se osiguralo da utvrđena kaznena djela budu kažnjiva učinkovitim, razmjernim i

[20] Sporazum CIS-a, čl. 3. st. 1. toč. (a) predviđa kriminaliziranje neovlaštenog pristupa računalnim podacima zaštićenim zakonom, gdje postupak rezultira uništenjem, blokiranjem, mijenjanjem ili kopiranjem podataka ili narušava funkcioniranje računala, računalnog sustava ili povezanih mreža.

[21] Nacrt Konvencije Afričke unije, poglavlje I., odjeljak 1., članak III-2: „Svaka država članica Afričke unije poduzet će zakonodavne mjere potrebne da se utvrdi kao kazneno djelo prijevarni pristup ili pokušaj pristupa cijelom ili dijelu računalnog sustava."

[22] Nacrt Direktive ECOWAS, članak 4.: „Prijevarni pristup računalnom sustavu djelo je kojim osoba prijevarno pristupi ili pokuša pristupiti cijelom ili dijelu računalnog sustava."

odgovarajućim sankcijama, koje uključuju i lišavanje slobode. Ta odredba pokazala se kao glavna slaba točka Konvencije s obzirom na to da zemlje potpisnice u slučaju težih napada sa štetom velikih razmjera nisu imale odgovarajuće osnove za teže kažnjavanje počinitelja.

Konvencija Lige arapskih država o suzbijanju informacijsko-tehnoloških kaznenih djela člankom 6. stavkom 2. kao otežavajuće propisuje okolnosti da neovlašteni pristup dovodi do ukidanja, izmjene, izobličenja, kopiranja, premještanja ili uništenja spremljenih podataka, elektroničkih instrumenta, sustava i komunikacijskih mreža te do štete korisnicima ili do stjecanja tajnih podataka vlade.[23]

Na nacionalnoj razini najčešće su otegotne okolnosti ostvarenje financijske koristi, ometanje rada sustava, uništenje ili zamjena podataka, pristup trećem računalu, prouzročenje znatne štete, prouzročenje javnog nereda, poticanje ili podupiranje terorizma, počinjenje djela u sklopu organizirane grupe, počinjenje djela s elementima nasilja. Najveći broj država kao otežavajuće okolnosti prepoznaje neovlašteni pristup računalnom sustavu države ili sustavu povezanom s radom kritične infrastrukture kao što su banke, telekomunikacije, zdravstvene ustanove i sl. U takvim slučajevima treba voditi računa o preklapanju kaznenih djela.[24]

Kazneno djelo neovlaštenog pristupa opisano je u članku 266. Kaznenog zakona. Za postojanje kaznenog djela dovoljan je sam neovlašteni pristup pa nisu postavljeni nikakvi dodatni uvjeti. Štoviše, tim kaznenim djelom ne sankcionira se samo neovlašteni elektronički pristup nego i slučajevi neovlaštenog fizičkog pristupa računalnom sustavu ili računalnim podacima.[25]

Za razliku od odredaba Konvencije VE ETS 185, Direktive 2013/40/EU i odredbe ranijeg KZ-a, čl. 266. aktualnog KZ-a RH od neovlaštenog pristupa, osim računalnog sustava, štiti i računalne podatke, koji se ne moraju nalaziti na računalnom sustavu, nego se mogu nalaziti i na nekom mediju izvan računalnog sustava. Međutim, u odnosu na odredbe Konvencije i Direktive, čl. 266. ne razlikuje posebno neovlašteni pristup cijelom ili dijelu računalnog sustava.

Ako uzmemo u obzir novu definiciju pokušaja iz čl. 34. Kaznenog zakona i činjenicu da neovlašteni pristup najčešće predstavlja pripremnu radnju, možemo zaključiti da je kažnjiva zona postavljena široko, čak šire od zahtjeva i obveza preuzetih članstvom u Vijeću Europe i Europskoj uniji. Stoga se može uputiti prigovor prekomjerne

[23] Arab Convention on Combating Information Technology Offences (League of Arab States Convention), League of Arab States, 2010,

[24] Comprehensive Study on Cybercrime, UNODC - Ured za drogu i kriminal UN-a, 2013, dostupno na http://www.unodc.org/documents/organized-crime/UNODC_CCPCJ_EG.4_2013/CYBERCRIME_STUDY_210213.pdf (30. 9. 2014.), str. 84 i 85.

[25] Turković, K.; Novoselec, P.; Grozdanić, V.; Kurtović Mišić, A.; Derenčinović, D.; Bojanić, I.; Munivrana Vajda, M.; Mrčela, M.; Nola, S.; Roksandić Vidička, S.; Tripalo, D.; Maršavelski, A., *op. cit.,* str. 129.

kriminalizacije, i to osobito uzimajući u obzir odredbu čl. 3. Direktive, koja propisuje kršenje sigurnosnih mjera kao minimalni uvjet za kriminalizaciju.

3.1.2. Neovlašteno ostajanje u informacijskom sustav

Situacija u kojoj osoba ostaje u informacijskom sustavu i nakon isteka ovlaštenja prepoznata je jednako ozbiljnom prijetnjom kao i neovlašteni pristup. Nekoliko međunarodnih instrumenata stoga propisuje neovlašteno ostajanje u informacijskom sustavu kao kazneno djelo. Nacrt Direktive Ekonomske zajednice država zapadne Afrike (ECOWAS) u borbi protiv kibernetičkog kriminaliteta u čl. 5. propisuje kao kazneno djelo prijevarno ostajanje ili pokušaj ostajanja u cijelom ili dijelu informacijskog sustava.[26] Sličnu definiciju možemo pronaći i u čl. 5. st. 1. modela zakonskog teksta o kibernetičkom ili e-kriminalitetu ITU/CARICOM/CTU, koji ostavlja mogućnost državama da ne kriminaliziraju ostajanje u sustavu ukoliko postoje drugi djelotvorni lijekovi. Većina međunarodnih instrumenata, među kojima i nama najvažnije Konvencija VE ETS 185 i Direktiva 2013/40/EU, ne pokriva ovo područje.

Na nacionalnoj razini također samo manji broj država prepoznaje neovlašteno ostajanje u informacijskom sustavu kao kazneno djelo. Neovlašteno ostajanje u informacijskom sustavu može biti propisano kao zasebno kazneno djelo ili obuhvaćeno kaznenim djelom neovlaštenog pristupa. Ostajanje u informacijskom sustavu znači da osoba još ima pristup sustavu, primjerice ostaje prijavljena na sustavu ili poduzima neke radnje u sustavu nakon isteka autorizacije. Činjenica da osoba ima teoretske mogućnosti prijaviti se na informacijski sustav neće biti sama po sebi dovoljna.[27] Kazneni zakon RH ne poznaje kazneno djelo neovlaštenog ostajanja u računalnom sustavu.

3.1.3. Neovlašteno pribavljanje računalnih podataka

Prema odredbama Konvencije VE ETS 185, drugo temeljno kazneno djelo protiv informacijskog sustava nakon nezakonitog pristupa opisanog u članku 2. jest kazneno djelo nezakonitog presretanja opisano u čl. 3. Između ta dva kaznena djela, međutim, postoji velik prostor za zlouporabe koje mogu ugroziti računalne sustave. Osim neovlaštenog ostajanja u informacijskom sustavu iz prethodnog poglavlja, takvo je i djelo neovlaštenog stjecanja računalnih podataka. Dok se kazneno djelo neovlaštenog presretanja odnosi, kao što ćemo kasnije vidjeti, na presretanje podataka u prijenosu, ostaje nejasno definirano područje u kojem osoba pribavlja podatke koji nisu u prijenosu, a da se radi o ovlaštenom pristupu računalnom sustavu, ili računalne podatke koji se ne nalaze u računalnom sustavu i ne predstavljaju dio sustava prema definiciji računalnog sustava. Primjerice, ukoliko se radi o računalu koje se nalazi na popravku kod servisera, ako on kopira podatke, ili ukoliko se radi o zlonamjernom zahvatu ovlaštenih službenih

[26] Nacrt Direktive ECOWAS, članak 5.: „Prijevarno ostajanje u računalnom sustavu djelo je kojim osoba prijevarno ostane ili pokuša ostati u cijelom ili dijelu računalnog sustava“, str. 4.
[27] Understanding Cybercrime: Phenomena, Challenges and Legal Response, *op. cit.* (bilj. 19.), str. 182.

osoba u računalne podatke koji se nalaze na sustavu kojem imaju pristup. S obzirom na važnost podataka pohranjenih na računalnom sustavu, potrebno je ocijeniti potrebu kaznenopravne zaštite. Kako je većina međunarodnih i nacionalnih instrumenata rađena po uzoru na Konvenciju VE ETS 185, takve su odredbe vrlo rijetke ili ograničene na teže slučajeve.

Kao primjer na nacionalnoj razini najcitiranija je odredba § 202a njemačkog Kaznenog zakona[28] Špijuniranje podataka, iz glave XV. Povreda privatnosti, koja se odnosi na onoga tko za sebe ili drugoga nezakonito pribavi podatke koji mu nisu namijenjeni i koji su posebno zaštićenih od neovlaštenog pristupa ukoliko zaobiđe zaštitu. Ova odredba odnosi se na one podatke koji su spremljeni ili preneseni elektronički ili magnetski ili na drugi način, a da nisu odmah percipirani. Kazneno djelo špijuniranja podataka koje se sastoji od pribavljanja podataka njemački kazneni zakon razlikuje od kaznenog djela presretanja podataka opisanog u § 202b.

Slično rješenje nalazimo u članku 8. Model zakonskog teksta o kibernetičkom ili e-kriminalitetu ITU/CARICOM/CTU, kao i članku 1831. Kaznenog zakona Sjedinjenih Američkih Država, ali koji se odnosi na točno određene važne podatke.[29]

Hrvatski kazneni zakon ne sadrži takve posebne odredbe o kriminalizaciji pribavljanja računalnih podataka, ukoliko se ne radi o općim odredbama o zaštiti autorskih prava, osobnih podataka te odredbama o odavanju poslovne, službene ili druge tajne.

3.1.4. Neovlašteno presretanje računalnih podataka

Za razliku od klasičnog prijenosa i dostave pošiljaka, uporaba informacijsko-telekomunikacijskih tehnologija uključuje brojne pružatelje usluga i mjesta na kojim se podaci mogu presresti. Stoga je zbog specifičnosti tehnologije, uz postojeća kaznena djela povrede privatnosti, uvedeno i posebno kazneno djelo neovlaštenog presretanja računalnih podataka s računalnim podatkom u prijenosu kao pravnim dobrom. Kriminalizacijom neovlaštenog presretanja zaštita se širi s podataka koji se nalaze u računalnom sustavu i na podatke u prijenosu. Podaci koji se štite korporativni su podaci, osobni podaci, podaci o broju kreditnih kartica, brojevi socijalnog osiguranja, lozinke, pristupne šifre, brojevi bankovnih računa i sl.[30]

Ovo kazneno djelo, uz ranije opisano kazneno djelo neovlaštenog pribavljanja podataka, predstavlja tzv. kompjutersku špijunažu. Mnogi međunarodni i nacionalni instrumenti sadrže posebne odredbe o kriminalizaciji kaznenog djela neovlaštenog presretanja.

---

[28] Strafgesetzbuch, § 202a Ausspähen von Daten, dostupno na http://www.gesetze-im-internet.de/stgb/index.html (30. 9. 2014.).

[29] United States Code, § 1831 dostupno na http://uscode.house.gov/browse/prelim@title18/part1&edition=prelim (30. 9. 2014.).

[30] Understanding Cybercrime: Phenomena, Challenges and Legal Response, *op. cit.* (bilj. 19), str. 184-186.

Nacionalni instrumenti koji ne sadrže posebne odredbe primjenjuju postojeće odredbe o nezakonitom prisluškivanju i snimanju, odnosno povredi tajnosti dopisivanja. To je moguće stoga što nezakonito presretanje može služiti kako zaštiti privatnosti tako i zaštiti integriteta računalnih podataka ili i jednom i drugom.

Navedeno kazneno djelo propisano je čl. 3. Konvencije VE te preuzeto u brojne druge instrumente kojima je kao najvažniji međunarodni instrument u borbi protiv kibernetičkog kriminaliteta poslužilo kao model. Prema obrazloženju,[31] cilj je ove odredbe izjednačavanje zaštite elektroničkog prijenosa sa zaštitom govorne komunikacije od neovlaštenog prisluškivanja i snimanja, koja je već postojala u nacionalnim zakonodavstvima. Njegova primjena ograničena je na presretanje prijenosa podataka tehničkim sredstvima, odnosno na pribavljanje podatka za vrijeme prijenosa. Stoga se članak ne može primijeniti na podatke koji nisu u prijenosu, kao primjerice pribavljanje podataka koji se nalaze pohranjeni na tvrdom disku. Iako se u obrazloženju naglašava da se prijenos podataka može odvijati i unutar pojedinog sustava (primjerice od CPU prema ekranu ili printeru), između dva računalna sustava koji pripadaju istoj osobi, između dva računala ili računala i osobe (primjerice, preko tipkovnice), upitno je mogu li se odredbe čl. 3. primijeniti i na slučajeve kad počinitelj sam upravlja prijenosom podataka. Ukoliko počinitelj pristupi sustavu i upotrijebi ga za kopiranje podataka na vanjski disk, tada njegova radnja dovodi do prijenosa podataka, međutim, takva radnja nije presretanje, nego iniciranje prijenosa.

Smatra se da su podaci u prijenosu sve dok nisu došli do krajnjeg odredišta, bilo sustava bilo primatelja. Podaci se mogu smatrati podacima u prijenosu i sve dok primatelj ne ostvari pristup tim podacima. Razlikovanje je bitno s obzirom na privremenu pohranu podataka prilikom izvršenja protokola. Pravni sustavi nekih zemlja i neki međunarodni instrumenti radi pravne sigurnosti pojam prijenosa podataka posebno određuju, pa tako i Konvencija o kibernetičkom kriminalu u članku 1. točki d).

Da bi postojalo kazneno djelo, potrebno je da prijenos bude nejavan, odnosno povjerljiv. Razlikovanje javnog od nejavnog prijenosa ne ovisi o prirodi podataka koji se prenose, nego o prirodi prijenosa, pa se može raditi o kaznenom djelo i ako se radi o javnim podacima, ali stranke žele komunicirati tajno. Jednako tako uporaba javne mreže automatski ne isključuje nejavnu komunikaciju. Da bi postojalo kazneno djelo, presretanje mora biti počinjeno s namjerom i mora se raditi o neovlaštenom presretanju. Prema obrazloženju uz Konvenciju, o ovlaštenom presretanju radilo bi se ukoliko se radi o naputku ili ovlaštenju sudionika prijenosa, ovlaštenom testiranju ili zaštitnim mjerama odobrenima od strane sudionika u komunikaciji, ovlaštenjima koja proizlaze iz odredaba kaznenog prava te ukoliko se radi o pitanju nacionalne sigurnosti. U hrvatskom kaznenom zakonodavstvu kazneno djelo neovlaštenog presretanja računalnih podataka opisano je u čl. 269. i u potpunosti je usklađeno s odredbama Konvencije o kibernetičkom kriminalu.

[31] *Explanatory Report to the Convention on Cyber Crime*, *op. cit.* (bilj. 1), alineja 51-59.

3.1.5. Ometanje rada računalnog sustava

Nacionalna kaznena zakonodavstva mogu se naći u problemu ako pokušavaju primijeniti tradicionalne kaznene odredbe o oštećenju materijalnih stvari na oštećenje ili ometanje računalnih sustava i računalnih podataka s obzirom na nematerijalnu komponentu računalnog sustava i neopipljivost računalnih podataka. Ometanje rada računalnog sustava kao jedno od kaznenih djela računalne sabotaže nije u svim zemljama propisano kao kazneno djelo. U onim zemljama u kojima je propisano kao kazneno djelo moguće je da je propisano kao posebno računalno kazneno djelo ili je obuhvaćeno tradicionalnim odredbama, a moguće su i kombinacije tradicionalnih odredaba s odredbama posebnog kaznenog djela računalnog kriminaliteta. Većina nacionalnih odredaba pokriva ometanje računalnog sustava, dok je manji dio ograničen na računalne mreže ili računalo. Time se domet odredaba znatno sužava pa mogu, primjerice, biti isključeni slučajevi sabotaže računalnog sustava koji nije umrežen ili slučajevi napada na druge uređaje kao što su mrežni usmjerivači virusima ili DDOS napadima.[32]

Ondje gdje je ometanje rada računalnog sustava propisano kao posebno kazneno djelo moguće je da je ono jasno odvojeno od kaznenog djela oštećenja računalnih podatka, moguće je da su oba kaznena djela opisana u istom članku ili pak postoji mogućnost da je granica između ta dva kaznena djela ostala nejasna. Na međunarodnoj razini većina multilateralnih instrumenata stoga i zahtijeva odvajanje odredaba o sabotaži računalnog sustava od sabotaže računalnih podataka, dok, primjerice, Konvencija o suzbijanju informacijsko-tehnološkog kriminaliteta Lige arapskih država ne predviđa kriminalizaciju ometanja sustava kao samostalno kazneno djelo.

Klasični oblici ometanja sustava koje prepoznaje većina pravnih sustava jesu mijenjanje, brisanje i prenošenje podataka. Šira definicija može obuhvatiti ne samo manipulaciju podacima nego i prekidanje električnog napajanja, uzrokovanje elektromagnetskih smetnja ili kvarenje sustava bilo kojim sredstvom.[33] Lista radnja koju koristi Konvencija VE ETS 185 konačna je i obuhvaća unošenje, prenošenje, oštećivanje, brisanje, kvarenje, mijenjanje ili činjenje neuporabljivih računalnih podataka. Unošenje kao način počinjenja ne definira se posebno ni Konvencijom ni u obrazloženju uz nacrt. S obzirom na to da se pojavljuje zajedno s pojmom prenošenje podataka, unos bi obuhvaćao korištenje fizičkog sučelja, dok bi prenošenje obuhvaćalo daljinski prijenos podataka.

Pojmovi oštećenje i kvarenje prema obrazloženju uz Konvenciju preklapaju se, a predstavljaju negativnu izmjenu integriteta podatka i programa. Brisanje predstavlja uklanjanje podatka iz medija za pohranu. Brisanjem se podaci uništavaju i postaju neprepoznatljivi. Pojam *suppresing*, koji ćemo detaljnije obrazložiti u nastavku, prema obrazloženju Konvencije, označava radnju koja negativno utječe na dostupnost podataka

[32] Comprehensive Study on Cybercrime, *op. cit.* (bilj. 24), str. 88-92.
[33] Commonwealth Model Law on Computer and Computer Related Crime, London, 2002, dostupno na: https://www.commonwealthcybercrimeinitiative.org/wp-content/uploads/2013/01/Commonwealth-Model-Law-2002.pdf (30. 9. 2014.) čl. 7.

osobi koja ima pristup mediju gdje je informacija pohranjena. Mijenjanje obuhvaća modificiranje podataka, a da se nužno ne umanjuje njihova uporabljivost.[34] Kao nužan element u nekim slučajevima propisuje se šteta ili gubitak prouzročen kaznenim djelom ili pak šteta predstavlja kvalifikatorni element.

Konvencija VE zahtijeva inkriminiranje ozbiljnog ometanja sustava, a Direktiva 2013/40/EU da se ne inkriminiraju lakši slučajevi. Nacionalnim zakonodavstvima propuštena je diskrecijska ocjena o tome kada će se raditi o ozbiljnom ili lakšem slučaju ometanja. U odnosu na Konvenciju VE, Direktiva EU 2013/40/EU obuhvaća kao alternativu i prekidanje funkcioniranja informacijskog sustava. Druga je uočljiva razlika da Direktiva predviđa mogućnost da se sustav može ometati i onemogućivanjem pristupa podacima. Takav učinak može imati i Konvencija, iako to izravno ne propisuje, ako se originalni pojam, koji na engleskom jeziku glasi *suppresing*, protumači u najširem smislu, kako ga je protumačila i sama ekspertna grupa na izradi Nacrta Konvencije. Službeni prijevod pojma *suppresing* za potrebe Konvencije glasi „činjenje neuporabljivim računalnih podataka", a za potrebe Direktive „prikrivanje računalnih podataka", što dodatno čini složenim primjenu i tumačenje. Jednako tako, za prijevod na hrvatski jezik za potrebe Konvencije pojam *deteriorating* preveden je kao kvarenje, a za potrebe Direktive kao uništavanje.

Nomotehnički u članku 267. Kaznenog zakona RH taj je problem riješen izbjegavanjem opisivanja načina počinjenja kaznenog djela, no, s druge strane, a imajući u vidu skromnu judikaturu i iskustvo, ostavljen je širok prostor za diskrecijsku ocjenu domaćih tijela vlasti u okviru ranije spomenuta četiri moguća opsega pojma, pa i daleko izvan toga, s rizikom prekomjerne kriminalizacije.

Nadalje, sam pojam *hindering* za potrebe Konvencije preveden je na hrvatski kao sprječavanje funkcioniranja, a za potrebe Direktive kao ometanje funkcioniranja, dok Kazneni zakonu RH govori o onemogućivanju ili otežavanju rada ili korištenja. Model zakonskog teksta o kibernetičkom ili e-kriminalitetu ITU/CARICOM/CTU u članku 3. posebno definira pojam *hindering*.

Oblik krivnje koji se traži u većini slučajeva jest namjera, međutim, neki sustavi traže i posebnu namjeru, prijevarnu ili usmjerenu na onemogućivanje rada sustava. U manjem broju država moguće je počiniti kazneno djelo ometanja rada računalnog sustava i iz nehaja, opravdavajući to činjenicom da je lakše nehajno omesti računalni sustav nego oštetiti materijalni objekt ili imovinu, radi čega računalni sustav treba posebnu zaštitu, kao što je to slučaj sa čl. 7. *Commonwealth Model Law on Computer and Computer Related Crime*, spomenutim u bilješci broj 57. U tom bi slučaju, primjerice, i nenamjerno presijecanje naponskog kabla računalnog sustava moglo dovesti do kaznene odgovornosti. Na kraju treba imati na umu da je ometanje sustava samo jedan od načina

[34] Understanding Cybercrime: Phenomena, Challenges and Legal Response, *op. cit.* (bilj. 19), str. 189-192.

manipulacije sustava kojim se onemogućava ili otežava rad ili korištenje te se postavlja pitanje kriminalizacije i drugih oblika manipulacija koji nemaju za posljedicu ometanje.

Kazneno djelo ometanja računalnog sustava u hrvatskom kaznenom pravu opisano je u članku 267. Kaznenog zakona. U odnosu na ranije odredbe, došlo je do značajne izmjene u dijelu koji se odnosi na oblik krivnje. Dok se ranije tražilo da djelo bude počinjeno s ciljem, što je upućivalo na izravnu namjeru, trenutno važeći Kazneni zakon ne postavlja taj uvjet pa se kazneno djelo može počiniti i s neizravnom namjerom, čime se domet odredaba znatno proširio. Ostale su odredbe neizmijenjene. Međutim, ni prethodni, a ni trenutno važeći Kazneni zakon nije usvojio pravno tehnička rješenja opisana u odredbama Konvencije VE ETS 185 niti ona opisana u Direktivi EU 2013/40/EU. Dok članak 5. Konvencije i članak 4. Direktive taksativno navode načine na koje se sustav može omesti, i to isključivo utjecajem na podatke, odredba Kaznenog zakona ne sadrži posebne odredbe o načinu počinjenja djela te je samim time i šira jer osim ometanja sustava manipulacijom podataka obuhvaća i druge vrste manipulacija, uključujući i oštećenje ili uništenje hardvera ili druge infrastrukture. U tom dijelu dolazi do preklapanja s kaznenim djelima oštećenja tuđe stvari te se otvara pitanje prekomjerne kriminalizacije.

3.1.5.1. *Spam*

Spamovi predstavljaju neželjene poruke e-poštom. Procjenjuje se da više od 70 % ukupnog prometa e-poštom otpada na *spamove*, čak i do 95 %. Kod *spamova* se prije postavlja pitanje pristanka nego li pitanje sadržaja poruke. Međutim, problem *spamova* veći je od samog ometanja korisnika. *Spamovi* iskorištavaju resurse sustava, utječu na propusnost, ispunjavaju kapacitete servera, koriste mrežnu infrastrukturu, predstavljaju ulaznu točku za širenje virusa i *phishing*-napade na pristupne šifre i povjerljive informacije. Stoga se *spamovi* mogu povezati s ometanjem sustava i podataka, odnosno s ugrožavanjem cjelovitosti i dostupnosti sustava i podataka.

Dva multilateralna neobvezujuća instrumenta, COMESA u članku 19. Nacrta modela zakona i ITU/CARICOM/CTU u članku 15. Modela zakonskog teksta, propisuju kriminalizaciju, dok ni jedan obvezujući ne zahtijeva kriminalizaciju.[35] Direktiva o privatnosti i elektroničkim komunikacijama EU-a[36] u preambuli ističe da je nužno zabraniti uporabu lažnog identiteta ili lažnih povratnih adresa, odnosno brojeva prilikom slanja neželjenih poruka u svrhe izravnog marketinga (alineja 43). Dalje u čl. 13. regulira neželjenu komunikaciju te u stavku 3. zahtijeva od država članica da poduzmu odgovarajuće mjere kako bi osigurale da besplatne neželjene komunikacije u svrhu izravnog marketinga ne budu dopuštene, bilo bez pristanka pretplatnika kojih se to tiče

[35] Comprehensive Study on Cybercrime, *op. cit.* (bilj. 24), str. 95 i 96.
[36] Direktiva 2002/58/EZ o obradi osobnih podataka i zaštiti privatnosti u području elektroničkih komunikacija Europskog parlamenta i Vijeća, SL L 201, 31. 7. 2002.

bilo u svezi s pretplatnicima koji ne žele primati komunikacije. Međutim, odredba ne traži kriminalizaciju *spamova*, kao ni Direktiva 2013/40/EU.

Prema istraživanju UN-a, jedna trećina zemalja propisuje slanje ili kontrolu *spamova* kao kazneno djelo, a samo devet posto ih ima i posebnu odredbu za to kazneno djelo. U borbi protiv prijetnja koje proizlaze iz *spamova* koriste se i druge odredbe koje se odnose na kompjutorske viruse ili *phishing*-napade.[37] Konvencija VE ETS 185 ne kriminalizira posebno *spamove*, nego ima u fokusu ometanje računalnih sustava. Sastavljači u obrazloženju navode da bi kriminalizacija trebala obuhvatiti samo ozbiljno i namjerno ometanje. Odredbe o kriminalizaciji *spamova* za potrebe komparativne analize nalazimo i u HIPCAR-ovu Modelu zakona o kompjutorskom kriminalu u članku 15. te u Kaznenom zakoniku SAD-a u članku 1037.[38]

3.1.6. Oštećenje računalnih podataka

Načini počinjenja kaznenih djela ometanja računalnog sustava i oštećenja računalnih podataka, kako su određeni Konvencijom VE ETS 185 i Direktivom 2013/40/EU, u bitnom se dijelu preklapaju. Oba ta kaznena djela mogu se počiniti oštećenjem, brisanjem, kvarenjem, mijenjanjem ili činjenjem neupotrebljivim računalnih podataka. Šire poimanje kaznenog djela ometanja računalnih podataka prema nekim pravnim rješenjima može obuhvatiti i druge radnje, pa čak i unošenje ili prijenos podataka. Ovo kazneno djelo pojavilo se kako bi se ispunile pravne praznine i kako bi se računalnim podacima osigurala zaštita od oštećenja i uništenja kakvu uživaju fizički predmeti. Jedno od alternativnih rješenja jest da se pojam stvari ili dobara proširi i na računalne podatke, no uvijek će ostati nedorečenosti i prijepora. Kazneno djelo ometanje podataka u Konvenciji VE nalazimo u članku 4., a u Direktivi EU-a kazneno je djelo opisano u članku 5.

Prema studiji UN-a,[39] dio država za kažnjavanje ometanja računalnih podataka traži da je to ometanje imalo utjecaj na funkcioniranje računalnog sustava. Neke države uključuju kao nužan element kaznenog djela štetu ili gubitak, neke štetu ili gubitak uzimaju kao kvalifikatorni element, dok polovica ispitanih država za postojanje kaznenog djela ne postavlja nikakav dodatni uvjet.

Radi pravne sigurnosti bitno je pobliže odrediti pojedine pojmove. Prema Obrazloženju uz Konvenciju VE, brisanje predstavlja uklanjanje podatka iz medija za pohranu. Brisanjem se podaci uništavaju i postaju neprepoznatljivi, kao, primjerice, materijalni predmeti. Prema tome, podaci se mogu izbrisati na različite načine. Stavljanje podataka u virtualnu kantu za smeće ne predstavlja uklanjanje podataka s tvrdog diska. Čak i pražnjenje kante ne mora odmah nužno značiti i trajno uklanjanje podataka. Stoga je

[37] Comprehensive Study on Cybercrime, *op. cit.* (bilj. 24), str. 95.
[38] United States Code, § 1037., dostupno na http://www.gpo.gov/fdsys/pkg/USCODE-2011-title18/pdf/USCODE-2011-title18-partI-chap47-sec1037.pdf (1. 10. 2014.).
[39] Comprehensive Study on Cybercrime, *op. cit.* (bilj. 24.), str. 89.

neodređeno isključuje li mogućnost povratka podataka primjenu kaznenih odredaba o oštećivanju podataka.

Da bi se radilo o kaznenom djelu prema Konvenciji, počinitelj mora poduzimati opisane radnje neovlašteno. Osim ranije spomenutih situacija, kao što su testiranje sustava i posjedovanje odobrenja, neće se raditi o neovlaštenom ometanju podataka i u slučaju modificiranja podataka u svrhu anonimne komunikacije putem *remailera* ili kriptiranja jer su te radnje poduzete u svrhu zaštite privatnosti, a samim time i s ovlaštenjem.[40] Gotovo sve države i međunarodne organizacije zahtijevaju da je djelo počinjeno s namjerom. Izuzetak je Model zakona zemalja Commonwealtha, koji u članku 6. predviđa da ometanje podataka može biti počinjeno i nehajno. U stavku drugom članka 6. Modela jasno se navodi da ometanje podataka može imati čak i samo privremeni učinak.

Kazneno djelo oštećenja računalnih podataka u hrvatskom kaznenom pravu opisano je u članku 268. KZ-a RH. U naslovu kaznenog djela koristi se izraz oštećenje, iako službeni prijevodi i Konvencije VE ETS 185 i Direktive 2013/40/EU glase ometanje. Analizom kaznenih djela oštećenja računalnih podataka i ometanja računalnog sustava može se zaključiti da ne prate ideju izraženu u spomenutim međunarodnim izvorima, što dovodi do preklapanja i poteškoća u primjeni. Iako bi se kazneno djelo ometanja sustava trebalo odnositi na sustav, uključujući komunikaciju, odnosno programe i podatke koji služe za potrebe njegova rada, korištenja, zaštite i održavanja, u definiciju su dodani i onemogućavanje ili otežavanje rada i korištenje i ostalih računalnih podataka i programa. U tom dijelu ometanje sustava preklapa se s kaznenim djelom oštećenja podataka.

Nadalje, ostaje otvoreno pitanje ovlaštenog pristupa sustavu i zlonamjernog korištenja resursa sustava, pa i podataka bez ometanja sustava, kopiranja podataka koji nisu u prijenosu, korištenja podataka bez njihova oštećivanja i sl. Sve navedeno upozorava na potrebu za reformom i doradom sustava zaštite ICT-a, osobito kad je u pitanju kritična nacionalna infrastruktura. U slučajevima oštećenja podataka i ometanja sustava potrebno je držati se osnovnih ideja izraženih u obvezujućim međunarodnim izvorima.

3.2. Računalna kaznena djela

Druga skupina kaznenih djela koja čine grupu kaznenih djela kibernetičkog kriminala jesu računalna kaznena djela. U odnosu na preostale tri skupine, koje su određene prema skupnom užem zaštitnom objektu, skupina računalnih kaznenih djela određena je prema *modusu operandi*, odnosno sredstvu počinjenja. Najvažnija iz skupine jesu kaznena djela računalnog krivotvorenja i računalne prijevare. U istu skupinu Međunarodna telekomunikacijska unija (ITU) uvrštava i *phishing,* krađu identiteta te zlouporabu naprava.[41] Za računalna kaznena djela bitno je da trebaju računalni sustav kao sredstvo počinjenja te da postoje i paralelna tradicionalna kaznena djela kojim se štite iste ili slične

[40] *Explanatory Report to the Convention on Cyber Crime*., *op. cit.* (bilj. 1.), komentar uz čl. 4., alineja 60-64.
[41] Understanding Cybercrime: Phenomena, Challenges and Legal Response, *op. cit.* (bilj. 19), str. 29.

vrijednosti u materijalnom obliku od napada klasičnim sredstvima. Direktiva 2013/40/EU o napadima na informacijske sustave ne propisuje računalna kaznena djela.

3.2.1. Računalno krivotvorenje

Pravno dobro koje se štiti kaznenim djelom računalnog krivotvorenja jest vjerodostojnost isprave u digitalnom obliku. Ono pokriva manipulaciju digitalnim dokumentima, odnosno podacima. Na međunarodnoj i regionalnoj razini šest instrumenata sadrži odredbe o računalnom krivotvorenju.[42] U obrazloženju uz članak 7. Konvencije VE ETS 185 o računalnom krivotvorenju navodi se da je cilj kriminalizacije bio izraditi djelo koje će biti pandan krivotvorenju materijalnih dokumenata, a s ciljem popunjavanja pravnih praznina povezanih s tradicionalnim poimanjem krivotvorenja. Manipulacija digitalnim podacima može imati iste ozbiljne posljedice kao i tradicionalno kazneno djelo. Računalno krivotvorenje u osnovi stoga obuhvaća izradu ili izmjenu pohranjenih podatka tako da oni dobiju drugu vrijednost u pravnom prometu koji se temelji na vjerodostojnosti podataka.

Tradicionalno poimanje krivotvorenja u pravilu podrazumijeva postojanje pisane isprave ili predmeta u materijalnom obliku i vizualnu prezentaciju, dok digitalni podaci zahtijevaju računalnu obradu i prezentaciju.

Posebno se naglašava u obrazloženju da dogmatska struktura nacionalnih pravnih sustava jako varira, od koncepta utemeljenog na autentičnosti autora do koncepta utemeljenog na istinitosti izjave sadržane u ispravi. Usuglašeno je da se obmana vjerodostojnosti odnosi u najmanju ruku na autentičnost izdavatelja, bez obzira na točnost ili istinitost sadržaja. Međutim, stranke mogu ići i dalje i pojmom vjerodostojnosti obuhvatiti i istinitost podataka.

Odredba o krivotvorenju jednako pokriva javne i privatne isprave koje imaju vrijednost za pravne odnose. Dakle, ova odredba ne štiti isprave koje nemaju vrijednost za pravne odnose. Objekt napada ovdje je računalni podatak, neovisno o tome je li odmah lako čitljiv ili shvatljiv. Neovlašteni unos, prema mišljenju sastavljača Konvencije, točnih ili netočnih podataka predstavlja situaciju jednaku izradi lažne isprave. Naknadne promjene (modifikacije, varijacije, parcijalne izmjene), brisanja (uklanjanje podataka s nositelja podataka) ili činjenje podataka neuporabljivim (zadržavanjem/prikrivanjem) odgovara krivotvorenju materijalne isprave. Ipak, za postojanje kaznenog djela ne traži se samo poduzimanje neke od spomenutih radnja na podacima nego i da te radnje rezultiraju nevjerodostojnim podacima.

U drugim pravnim izvorima mogu se pronaći rješenja koja zahtijevaju da manipulacija na podacima bude povezana s ometanjem sustava. Člankom 7. Konvencija dopušta

[42] Comprehensive Study on Cybercrime, *op. cit.* (bilj. 24), Dodatak 3., str. 268.

državama strankama da kaznenu odgovornost vežu na postojanje prijevarne ili druge nepoštene namjere.

Na nacionalnoj razini situacija s kriminalizacijom varira ovisno o tome postoje li specifična računalna kaznena djela o krivotvorenju ili se isto pokriva tradicionalnim odredbama ili se pak koriste oba rješenja. Razlika proizlazi iz mogućnosti učinkovitog proširenja tradicionalnih odredaba o krivotvorenju i na računalne podatke. Tako je moguće da se definicija isprave dopuni i računalnim podacima ili pak da se bez dopune zakona koristi tradicionalna definicija, ukoliko je moguće da se ona protumači na način da obuhvati digitalne isprave, digitalni potpis i podatke. Tipična dva elementa kaznenog djela računalnog krivotvorenja na nacionalnoj razini jesu izmjena ili manipuliranje računalnim podacima i posebna namjera uporabe podataka kao da su vjerodostojni.[43]

Kazneno djelo računalnog krivotvorenja u hrvatskom kaznenom pravu izrađeno je po uzoru na članak 7. Konvencije, a opisano je u čl. 270. KZ-a RH. U odnosu na ranije kaznene odredbe, ispušten je računalni program kao objekt napada te je dodan nov način počinjenja kroz formulaciju činjenja računalnih podataka nedostupnima.

3.2.2. Računalna prijevara

Računalna prijevara podizanjem gotovog novca iz bankomata s ukradenom, a u nemalom broju slučajeva i krivotvorenom bankovnom karticom i odgovarajućim tajnim osobnim brojem najzastupljeniji je oblik računalnog kriminaliteta u RH.[44]

Kao i kod računalnog krivotvorenja, neki pravni sustavi ne propisuju računalnu prijevaru kao zasebno kazneno djelo, nego kao običnu prijevaru. Glavna razlika između obične i računalne prijevare, gdje takva distinkcija postoji, jest u objektu napada. Kod klasične prijevare objekt je napada osoba koju počinitelj dovodi u zabludu ili održava u zabludi, dok je kod računalne prijevare objekt napada računalni sustav ili su to računalni podaci. Međutim, cilj je isti kako kod obične tako i kod računalne prijevare – stjecanje protupravne imovinske koristi.

Konvencija VE računalnu prijevaru opisuje u čl. 8. U obrazloženju uz Konvenciju navodi se da je cilj čl. 8. kriminalizacija svake neprikladne manipulacije podacima u obradi s namjerom ilegalnog prijenosa imovine. Kako bi svi mogući oblici manipulacije bili obuhvaćeni, temeljnim oblicima unošenju, mijenjanju, brisanju ili činjenju neuporabljivim računalnih podataka dodana je u točki 2. generalna klauzula koja se odnosi i na bilo kakvo ometanje funkcioniranja sustava. Tako da točka 2. obuhvaća i djela kao što su manipulacija hardverom, činjenje neuporabljivim ili prikrivanje ispisa, djela kojima se utječe na snimanje ili protok podataka ili djela kojima se utječe na slijed kojim su programi pokrenuti. Manipulacije koje predstavljaju računalnu prijevaru kriminaliziraju se samo

[43] Comprehensive Study on Cybercrime, *op. cit.* (bilj. 24), str. 97 i 98.
[44] Novoselec, P., , *Sudska praksa*, Hrvatski ljetopis za kazneno pravo i praksu vol. 15, broj 2/2008, str. 1166-1167.

ako je drugome prouzročen gubitak imovine, a počinitelj postupa s ciljem da sebi ili drugome pribavi protupravnu imovinsku korist. Pojam gubitak imovine u širem smislu uključuje novac i ekonomski vrijednu materijalnu i nematerijalnu imovinu. Prema čl. 8 Konvencije, djelo mora biti počinjeno neovlašteno. Zajednička trgovinska praksa usmjerena ostvarivanju ekonomske dobiti ne bi trebala biti obuhvaćena ovim djelom jer se ona provodi u skladu s pravom, kao što je, primjerice, aktivnost onesposobljavanja *web*-stranice temeljem uvjeta iz valjanog ugovora.

Računalna prijevara može se počiniti samo s namjerom. Opći element namjere odnosi se na prouzročenje štete na imovini drugoga manipulacijom ili ometanjem računalnog sustava. Specijalni element namjere pak se odnosi na prijevarnu ili drugu nepoštenu namjeru pribavljanja protupravne imovinske koristi sebi ili drugome. Stoga se ni ovdje ne zahtijeva kriminalizacija trgovačke prakse u pogledu tržišnog natjecanja, koja dovodi do ekonomske štete s jedne, a koristi s druge strane, jer se ne provodi s prijevarnom ili drugom nepoštenom namjerom. Tako, primjerice, korištenje programa za prikupljanje podataka radi uspoređivanja trgovina na internetu, pa čak i bez odobrenja trgovine čiju je stranicu *bot* posjetio, ne bi trebalo predstavljati kazneno djelo računalne prijevare.[45]

Kazneno djelo računalne prijevare u hrvatskom kaznenom pravu izrađeno je po uzoru na čl. 8. Konvencije, a opisano je u čl. 271. KZ-a RH. U odnosu na ranije kaznene odredbe, ispušten je računalni program kao objekt napada te samo korištenje sustava kao jedan od načina počinjenja. Međutim, u opis kaznenog djela dodani su novi načini počinjenja oštećenjem ili činjenjem nedostupnim računalnih podataka. U novom Kaznenom zakonu ispuštena je i odredba koja je propisivala kažnjavanje za postupanje s ciljem nanošenja štete drugom, a dodana je kvalifikatorna okolnost pribavljanja znatne imovinske koristi ili prouzročenja znatne štete.

3.2.3. Krađa identiteta

Krađa identiteta predstavlja prijevarno pribavljanje i uporabu identiteta druge osobe. Može biti počinjena bez uporabe tehničkih sredstava, ali i *online*, uporabom interneta. Iz tih je razloga i svrstana u grupu računalnih kaznenih djela koja, osim tradicionalnim sredstvima, mogu biti počinjena i sredstvima ICT-a. S obzirom na to da se socijalna i ekonomska interakcija preselila na mrežu i predstavlja prioritetna područja razvoja, podaci vezani za identitet osobe od krucijalnog su značenja. Paralelno s tim razvojem, mijenjalo se i poimanje pojma identiteta od više filozofskog deskriptivnog, koje obuhvaća skup osobnih karakteristika, prema identificiranju osobe na temelju brojčanih oznaka.

Općenito, krađa identiteta odvija se kroz tri faze. U prvoj počinitelj nabavlja informacije povezane s identitetom, primjerice napadom malicioznim softverom, korištenjem *phishing*-tehnike, socijalnim inženjeringom, krađom računala i sl. U drugoj fazi dolazi do

[45] *Explanatory Report to the Convention on Cyber Crime*, *op. cit.* (bilj. 1), komentar uz članak 8., alineja 86.-90.

raspolaganja podacima, posjedovanja i prijenosa, s ciljem da se uporabe u kriminalne svrhe, kao što je prodaja informacija o identitetu. U trećoj fazi podaci o identitetu koriste se kod počinjenja kaznenog djela, primjerice kod krivotvorenja osobnih isprava ili kod prijevara kreditnim karticama.[46]

Temeljem iznesenoga, dva su temeljna pristupa kriminalizaciji krađe identiteta. U prvom slučaju postoji posebno kazneno djelo koje kriminalizira djela pribavljanja, posjedovanja ili uporabe podatka o tuđem identitetu u kriminalne svrhe. U drugom slučaju kriminaliziraju se pojedine radnje koje spadaju u jednu od tri opisane faze kroz druga kaznena djela pa tako pribavljanje podataka može biti kriminalizirano kroz odredbe o neovlaštenom pristupu, zlouporabi naprava, neovlaštenom presretanju, ometanju podataka i dr., a neovlašteno posjedovanje i uporaba, primjerice, kroz kazneno djelo računalnog krivotvorenja.[47]

Najpoznatiji primjer jedinstvenog kaznenog djela krađe identiteta jest američki Kazneni zakonik, koji u člancima 1028(a)(7) i 1028A(a)(1) opisuje sve tri ranije spomenute faze. Kao drugi primjer može se navesti odredba članka 14. HIPCAR modela zakona o kompjutorskom kriminalu. Smjernicom broj 4. Komisije za tumačenje Konvencije VE ETS 185 o krađi identiteta i *phishingu* povezanom s prijevarom detaljno je obrazložen drugi pristup, s obzirom na to da Konvencija nema posebne odredbe o krađi identiteta.

Na razini nacionalnog zakonodavstva samo mali broj država propisuje posebno računalno kazneno djelo povezano s krađom identiteta, dok u nekima krađa identiteta i ne predstavlja kazneno djelo.[48] Ondje gdje takva odredba postoji najčešće se ne pokrivaju sve tri faze krađe identiteta. Tako ranije spomenuti članci američkog kaznenog zakonika ne pokrivaju baš sve aktivnosti vezane uz krađu identiteta. One ne pokrivaju situaciju gdje žrtva sama prosljeđuje podatke na inicijativu počinitelja, s obzirom na to da se počinitelja kažnjava za prijenos, a ne i za samo iniciranje prijenosa podataka o identitetu. Neke pak druge odredbe pokrivaju samo posjedovanje ili posjedovanje i uporabu ili pak samo uporabu. Neke pak idu i dalje te kriminaliziraju izradu lažnih osobnih podataka.

Direktiva 2013/40/EU u članku 9. stavku 5., uzimajući u obzir manjkavosti nacionalnih zakonodavstava na području krađe identiteta, propisuje da države članice poduzimaju potrebne mjere kojima osiguravaju da se, kada su kaznena djela ometanja sustava i ometanja podataka počinjena zlouporabom osobnih podataka druge osobe s ciljem zadobivanja povjerenja treće strane i uz nanošenje štete legitimnom vlasniku identiteta, ti elementi mogu smatrati otegotnim okolnostima, osim ako su te okolnosti već obuhvaćene drugim djelom kažnjivim prema nacionalnom pravu. U području zaštite

[46] T-CY Guidance Note # 4, Identity theft and phishing in relation to fraud, dostupno na http://www.coe.int/t/dghl/cooperation/economiccrime/Source/Cybercrime/TCY/TCY%202013/T-CY%282013%298REV_GN4_id%20theft_V10adopted.pdf (1. 10. 2014.), str. 3-5.
[47] Model zakonskog teksta o kibernetičkom ili e-kriminalitetu ITU/CARICOM/CTU, str. 33.
[48] Understanding Cybercrime: Phenomena, Challenges and Legal Response, *op. cit.* (bilj. 19), str. 100.

osobnih podataka Europska je komisija pokrenula inicijativu za donošenje Ugovora o zaštiti podataka za Europu.[49]

Kazneni zakon RH također ne poznaje posebno računalno kazneno djelo vezano za krađu identiteta, već se, prema smjernici 4. T-CY Komisije za tumačenje Konvencije VE, ono procesuira kroz odredbe različitih članaka, sa svim manjkavostima kojih smo se ranije dotaknuli. Međutim, sukladno Prijedlogu Direktive, u st. 2. čl. 273. KZ-a RH, koji se odnosi na Teška kaznena djela protiv računalnih sustava, programa i podataka, propisan je teži oblik kaznenih djela neovlaštenog pristupa, ometanja rada računalnog sustava, oštećenja računalnih podataka i neovlaštenog presretanja računalnih podataka, čime je pokriven samo dio radnja koje se mogu okarakterizirati kao krađa identiteta.

3.3. Zlouporaba naprava

Kaznenim djelom zlouporaba naprava kriminaliziraju se određene pripremne radnje poduzete radi počinjenja nekih od računalnih kaznenih djela. Softveri i drugi alati koji se koriste za počinjenje kaznenih djela u računalnom okruženju, kao i lozinke i pristupne šifre, postali su ilegalna roba na crnom internetskom tržištu.

Inkriminacija djela nailazi na brojne izazove. Najznačajniji je od njih različit pristup razgraničenju stadija pripremanja i pokušaja kaznenog djela. Drugi se odnosi na dvostruku ulogu sredstva, koja se mogu upotrijebiti kako u kriminalne tako i u nekriminalne svrhe. Inkriminacija pripremnih radnja nije nepoznata kod klasičnih kaznenih djela, primjerice kad su u pitanju pripremne radnje izrade i nabavljanja oružja i sredstava za počinjenje kaznenog djela.[50]

Zlouporaba naprava opisana je u članku 6. Konvencije ETS 185. Pojam „naprava“ prema obrazloženju uz Konvenciju odnosi se kako na hardver tako i na softverska rješenja namijenjena počinjenu nekog iz grupe kaznenih djela. Kao primjer softvera navode se virusi ili programi izrađeni ili prilagođeni za ostvarivanje neovlaštenog pristupa računalnom sustavu. Kompjutorske lozinke, pristupne šifre ili slični podaci ne izvode nikakve operacije, nego jednostavno predstavljaju pristupne kodove. Konvencija VE kriminalizira širok spektar radnja. Osim proizvodnje, kriminalizira se i prodaja, pribavljanje radi uporabe, uvoz, distribucija ili činjenje dostupnim na drugi način. Slična rješenja nalazimo i u dokumentima EU-a o pitanju povrede autorskih prava.[51]

Odredbe Konvencije ne odnose se samo na naprave koje su dizajnirane isključivo za olakšavanje počinjenja računalnog kriminaliteta nego i na naprave koje se inače koriste u legalne svrhe, kad ih počinitelj koristi s namjerom počinjenja nekog računalnog kaznenog

[49] Inicijativa za donošenjem novog Ugovora o zaštiti podataka za Europu, komunikacija dostupna na: http://europa.eu/rapid/press-release_IP-14-70_hr.htm (1. 10. 2014.)
[50] Comprehensive Study on Cybercrime, *op. cit.* (bilj. 24), str. 92-94.
[51] Direktiva 2001/29/EZ o usklađivanju određenih aspekata autorskog i srodnih prava u informacijskom društvu Europskog parlamenta i Vijeća, SL L 167, 22. 6. 2001., čl. 6.

djela iz grupe kaznenih djela protiv tajnosti, cjelovitosti i dostupnosti računalnih podataka. Sastavljači Konvencije u obrazloženju navode da bi ograničavanje samo na naprave koje su dizajnirane isključivo za počinjenje kaznenog djela bilo preusko i da bi moglo dovesti do nepremostivih teškoća dokazivanja u kaznenom postupku, čineći odredbu neprimjenjivom ili primjenjivom samo u rijetkim slučajevima.

Kao i u slučaju ostalih kaznenih djela iz Konvencije, ovo kazneno djelo moguće je počiniti samo s namjerom. Kao posebni element zahtijeva se namjera usmjerena na počinjenje kaznenih djela opisanih u člancima 2.-5. Za usporedbu, treba spomenuti da odredbe Modela zakona o kompjutorskom kriminalu zemalja Commonwealtha predviđaju kriminalizaciju čak i nehajne zlouporabe naprava. Za razliku od Konvencije VE, ne zahtijevaju svi multilateralni instrumenti ni specijalnu namjeru počinjenja točno određenih kaznenih djela, već je dovoljno da je naprava izrađena s primarnom svrhom počinjenja kaznenog djela. Kako bi izbjegli prekomjernu kriminalizaciju, HIPCAR-ov zakonski tekst o računalnom kriminalu u članku 10. predviđa da države mogu odlučiti kriminalizirati samo naprave koje bi se nalazile na popisu.

Jedno od drugačijih rješenja jest i da se kriminalizacija odnosi samo na maliciozne softvere, a ne i na naprave i na pristupne lozinke. Neki multilateralni instrumenti također dodatno pokrivaju naprave i predmete za počinjenje specifičnih kaznenih djela, kao što to, primjerice, propisuje Vijeće EU-a u okvirnoj odluci o borbi protiv prijevara i krivotvorenja povezanih s bezgotovinskim sredstvima plaćanja.[52]

U hrvatskom kaznenom pravu kazneno djelo zlouporabe naprave opisano je u članku 272. Kaznenog zakona. Zakonski tekst u skladu je s odredbama Konvencije VE ETS 185 i Direktive 2013/40/EU. U odnosu na Konvenciju VE postavljen je šire te obuhvaća i naprave koje se koriste za počinjene kaznenih djela računalne prijevare i računalnog krivotvorenja.

3.4. Teška kaznena djela protiv računalnih sustava, programa i podataka, sankcije i mjere

Jedan od prigovora Konvenciji o kibernetičkom kriminalitetu odnosio se na okolnost da ne osigurava odgovarajuću reakciju na najteže oblike napada na informacijske sustave. U skladu s tim, u situacijama u kojima je prouzročena šteta velikih razmjena, kao kod napada na Estoniju ili Gruziju, nije postojala odgovarajuća zakonska odredba koja bi osigurala učinkovitu, razmjernu i odvraćajuću sankciju počinitelju. Stoga su Direktivom 2013/40/EU posebno razrađene odredbe o sankcijama i, za razliku od Konvencije, detaljno propisane.

[52] Council framework decision of 28 May 2001 combating fraud and counterfeiting of non-cash means of payment, SL L 149, 2. 6. 2001., čl. 4.

Pri tome je posebna pozornost dana novim, posebno opasnim pojavnim oblicima napada kad je pogođen znatan broj računalnih sustava, primjerice stvaranjem i uporabom „botneta“, kad su napadi počinjeni u okviru zločinačke organizacije, kad je napadom prouzročena ozbiljna šteta ili je napad počinjen protiv informacijskog sustava ključne nacionalne infrastrukture, kao i zlouporabom podataka druge osobe.

Na sličan način u čl. 273. Kaznenog zakona RH predviđeni su i opisani kvalificirani oblici pod nazivom „Teška kaznena djela protiv računalnih sustava, programa i podataka“. Članak je usklađen s odredbama Prijedloga Direktive o napadima na računalne sustave. Također su u skladu s Prijedlogom Direktive usklađene i odredbe o sankcijama u svakom pojedinom članku.

4. ZAKLJUČAK

U kazneno zakonodavstvo Republike Hrvatske preuzete su odredbe koje proizlaze iz obveza utvrđenih Konvencijom o kibernetičkom kriminalu VE i Direktivom EU-a o napadima na informacijske sustave. Međutim, način na koji su preuzete pravno-tehnički slabi njihovu uporabnu vrijednost. Temeljni pojmovi, kao što su računalni podaci, programi, mreža, u bitnim dijelovima različito su prevedeni, protumačeni i kroz zakonski tekst međusobno različito postavljeni. Većina kaznenih djela kibernetičkog kriminala postavljena je šire od minimalnih okvira spomenutih međunarodnih izvora, dok su pojedina kaznena djela ostala nedorađena. Iako takva u radu opisana rješenja nisu zabranjena niti nepoznata na međunarodnoj razini, postavlja se pitanje njihove kriminalno-političke opravdanosti, poštivanja načela zakonitosti, prekomjerne kriminalizacije i standarda pravne zaštite i sigurnosti. S druge pak strane, uočljive su pravne praznine kad su u pitanju djela neovlaštenog ostajanja u računalnom sustavu i neovlaštenog pribavljanja računalnih podataka. Takva rješenja nisu usamljena i preslika su stvarnog stanja na području kriminalizacija napada na informacijske sustave na međunarodnoj razini.

S obzirom na ogroman doprinos informacijsko-komunikacijskih tehnologija razvoju društva, potrebno je slobode i prava koje ljudi imaju izvan kibernetičkog prostora osigurati i unutar kibernetičkog prostora, sa svim raspoloživim sredstvima, a kriminalizaciji napada pribjeći tek kao krajnjem sredstvu suzbijanja najtežih od njih. U tom pogledu kao prikladnije rješenje kod blažih oblika napada bilo bi uvođenje i prekršajne odgovornosti po uzoru na druga posebna područja, čime bi se otvorio prostor za detaljniju razradu složene terminologije i sveukupne problematike. Kod najtežih pojavnih oblika bit će potrebno popuniti ranije spomenute pravne praznine.

Za kraj, može se zaključiti da, bez obzira na pravni kontinuitet zaštite informacijskih sustava, programa i podataka u kaznenom zakonodavstvu Republike Hrvatske, i dalje ostaju otvorena pojedina pitanja koja su od važnosti za sveobuhvatno uređenje područja.

Summary

CRIMINAL-LAW PROTECTION OF COMPUTER SYSTEMS, PROGRAMS AND DATA

A large majority of countries around the world have agreed in principle on the need to criminalise the most serious cyber attacks, although there are different approaches to this issue at international and national levels. The most important international instrument to combat attacks against information systems, the Council of Europe Convention on Cybercrime of 2001, has over time proven to be insufficient, hence the European Parliament and the Council adopted a Directive on attacks against information systems, whose aim is to remove these shortcomings. The Republic of Croatia transposed the provisions of the Convention and of the proposed Directive into its new criminal legislation, and assumed the commitments arising therefrom. Since the adoption of the new Criminal Code has presented a unique opportunity to systematically regulate this area of criminalisation, this paper gauges the success of the new provisions, using comparative and other methods.

Keywords: *cybercrime, attacks against information systems, computer systems, computer programs, computer data*

Ivica Kokot, univ. spec. crim., attending postgraduate doctoral study at the Faculty of Law, University of Zagreb