RAČUNALNA PRIJEVARA U HRVATSKOM KAZNENOM PRAVU

Dr. sc. Igor Vuletić, docent
Tomislav Nedić, student V. godine
Pravni fakultet Sveučilišta u Osijeku

UDK: 343.72::004.7
Ur.: 18. lipnja 2014
Pr.: 1. listopada 2014.
Prethodno priopćenje

Sažetak

U ovom radu autori se bave problematikom računalne prijevare. Računalna prijevara, kao jedan od najučestalijih i najopasnijih oblika kibernetičkoga kriminala posljednjih godina sve više zaokuplja pažnju u komparativnoj literaturi i praksi. Osim toga, Konvencija o kibernetičkom kriminalu Vijeća Europe traži od potpisnica implementiranje neizravnog oblika računalne prijevare. Autori uvode po prvi put u hrvatsku kaznenopravnu literaturu pojmove izravna i neizravna računalne prijevara, kritički analiziraju oba oblika uz osvrt na hrvatsko i komparativno zakonodavstvo i praksu te daju svoje prijedloge za budućnost.

Ključne riječi: *prijevara, računalni sustav, kibernetski, oštećenik, zabranjena analogija, pokušaj.*

1. UVOD

Razvoj i napredak društva stalno donosi nove pojavne oblike kriminaliteta. Taj proces tradicionalno kazneno pravo stavlja pred mnoge izazove. Jedan od tih novih kaznenopravnih fenomena je i računalni kriminalitet, koji je posljednjih petnaestak godina u značajnom porastu. Pod pojmom računalnog kriminaliteta, za potrebe ovog rada, podrazumijevamo sva kaznena djela koja se tiču računalnih podataka.[1]

Računalni kriminalitet u sebi sadrži veliku potencijalnu opasnost. Ta opasnost, prije svega, proizlazi iz činjenice da je normalno funkcioniranje suvremenog društva praktički ovisno o stabilnoj i učinkovitoj računalnoj mreži. Stoga bilo kakvo ozbiljnije ugrožavanje računalne mreže može dovesti do kolapsa egzistencijalno važnih područja, poput komunikacijskog, vojnog, proizvodnog, financijskog, poreznog itd.[2]

1 Tako i Sieber, U. u Sieber/Brüner/Satzger/Heintschel-Heinegg (Hrsg.), Europäisches Strafrecht, Nomos, Baden-Baden, 2011., § 24, r. b. 1.
2 Ibid.

Temeljno obilježje računalnog kriminaliteta je nematerijalna priroda računalnih podataka kao objekta ovih kaznenih djela.[3] U situacijama u kojima nema posebnih propisa primjenjuju se opća načela kaznenog prava.[4] Ipak, spomenuta nematerijalna (virtualna) priroda, uz druge probleme kao što su složenost računalnog sustava, anonimnost korisnika, globalna računalna povezanost i dr. ukazuje na očiglednu potrebu za redefinicijom tradicionalnih kaznenopravnih koncepata.

Računalna prijevara jedan je od najčešćih oblika računalnog kriminaliteta. Zahvaljujući globalnoj rasprostranjenosti internet mreže, broj prijevara putem računala i računalnog sustava u stalnom je porastu i sa sve većim materijalnim posljedicama. Nabolji dokaz toj tvrdnji je činjenica da je ovaj oblik računalnog kriminaliteta postao i predmetom reguliranja međunarodnih dokumenata. Ipak, u hrvatskoj kaznenopravnoj literaturi ovaj kaznenopravni fenomen je do sada uglavnom bio zapostavljen, uz tek poneki fragmentarni osvrt.

Cilj je ovog rada po prvi put sustavno obraditi problematiku računalne prijevare. Poredbena literatura u pravilu čini razliku između dva oblika računalne prijevare. Tim ćemo putem poći i mi pa ćemo u nastavku teksta prikazati osnovne karakteristike obaju oblika i upozoriti na neke specifičnosti računalne prijevare u teoriji, zakonodavstvu i praksi. Primarni predmet našega interesa je hrvatsko kazneno pravo. No, na mjestima gdje to bude svrhovito, ukazat ćemo i na odgovarajuća rješenja iz poredbenog prava te poredbene literature i sudske prakse.

2. DVA OBLIKA RAČUNALNE PRIJEVARE

U kaznenom pravu izraz «računalna prijevara» može se shvatiti dvojako. S jedne strane, postoji, tzv. **izravna računalna prijevara**, koja se sastoji u obmanjivanju oštećenika koji je fizička osoba na način da se kao sredstvo obmanjivanja koristi računalni sustav. Tu se, dakle, radi o kaznenom djelu prijevare koje je specifično po sredstvu koje se koristi kako bi se oštećenika dovelo u zabludu i/ili održavalo u zabludi. S druge strane, moguća je i tzv. **neizravna računalna prijevara**, koja se sastoji u varanju samoga računalnog sustava. Drugim riječima, računalni sustav je objekt kaznenog djela. Tipičan primjer neizravne računalne prijevare je slučaj počinitelja koji pristupa bankomatu s tuđom karticom i podiže novac iako za to nije ovlašten. Tu se, dakle, radi o slučajevima u kojima počinitelj utječe na elektroničku obradu podataka kako bi sebi ili drugome pribavio protupravnu imovinsku korist.[5] Ovakvim se postupanjem posredno oštećuje treća

3 Ibid.

4 Na to ukazuje i Sieber, U., Verantwortlichkeit im Internet, Technische Kontrollmöglichkeiten und multimediarechtliche Regelungen, C. H. Beck`sche Verlagsbuchhandlung, München, 1999., str. 218.

5 Novoselec, P. i Bojanić, I., u Novoselec (ur.), Posebni dio kaznenog prava, Pravni fakultet Sveučilišta u Zagrebu, Zagreb, 2007., str. 240.

osoba koja ima vlast nad bankomatom (to će, u pravilu, biti banka).[6] Neizravni oblik računalne prijevare rezultat je novijeg razvoja kaznenog prava. Ustanovljen je čl. 8. Konvencije o kibernetičkom kriminalu Vijeća Europe (dalje: Konvencija) iz 2001. godine.[7]

U nastavku rada osvrnut ćemo se na oba oblika računalne prijevare. Prvenstveni predmet zanimanja ovog rada je računalna prijevara u hrvatskom zakonodavstvu i sudskoj praksi. Na mjestima gdje to bude svrhovito, ukazat ćemo i na neka od poredbenih rješenja te na stajališta strane teorije i sudske prakse.

2.1. Izravna računalna prijevara

Kako je već ranije napomenuto, izravni oblik računalne prijevare sastoji se u tome da počinitelj dovodi u zabludu ili održava u zabludi drugu osobu, koristeći pritom računalni sustav kao sredstvo obmane. Oštećenik je u ovom slučaju uvijek fizička osoba.[8]

Kod pristupanja normiranju ovog oblika računalne prijevare zakonodavac ima na raspolaganju dvije mogućnosti. Može predvidjeti poseban oblik prijevare ili može ostaviti praksi da ovakva ponašanja razmatra u okviru općeg kaznenog djela prijevare. Potonje rješenje, međutim, u sebi sadrži opasnost da se pojedini oblici prijevare, zbog svojih specifičnosti, ne mogu podvesti pod klasično kazneno djelo prijevare.[9] U nastavku ćemo razmotriti neke od najčešćih oblika prijevare fizičkih osoba putem računala.

Jedan od češćih oblika takvog postupanja je prijevara putem e-maila. Široku rasprostranjenost ovog oblika prijevare možda najbolje prikazuje činjenica da gotovo ne postoji korisnik interneta koji na svojem e-mailu barem jednom nije dobio poruku u kojoj se od njega ili nje traži dostavljanje podatka o broju svog bankovnog računa radi isplate određene neočekivane dobiti od igara na sreću i sl. Ovakva djela najčešće imaju međunarodni predznak, s obzirom na to da počinitelji

6 Pojmovi «izravna» i «neizravna» računalna prijevara su, za potrebe ovog rada, preuzeti iz komparativne literature na engleskom jeziku i prilagođeni hrvatskom jeziku. Literatura na engleskom jeziku razlikuje pojmove «direct computer fraud» i «indirect computer fraud». Usp. npr. Šepec, M., Slovenian Criminal Code and Modern Criminal Law Approach to Computer-related fraud, International Journal of Cyber Criminology, 2012., Vol. 6 (2), str. 986 i dalje.

7 Konvencija o kibernetičkom kriminalitetu: Članak 8. – RAČUNALNA PRIJEVARA *Svaka stranka će usvojiti zakonske i druge mjere potrebne kako bi se unutarnjim zakonodavstvom kaznenopravno sankcionirao namjerni čin neovlaštenog uzrokovanja štete na imovini drugoga: a. bilo kakvim unošenjem, mijenjanjem, brisanjem ili činjenjem neuporabljivima računalnih podataka, b. bilo kakvim ometanjem funkcioniranja računalnog sustava s prijevarnom ili nepoštenom namjerom neovlaštenog pribavljanja ekonomske koristi za sebe ili drugoga.*

8 Stajalište da oštećenik kod ovog oblika prijevare može biti samo fizička osoba logično proizlazi iz činjenice da se samo fizička osoba može dovesti u zabludu u klasičnom smislu. Za potonju činjenicu v. Novoselec, P., i Bojanić, I., u Novoselec, P., (ur.), op. cit., str. 240.

9 Na to upozorava i Šepec, M., op. cit., str. 992.

i žrtve dolaze iz različitih država pa to može stvoriti i probleme oko uspostavljanja kaznene vlasti i nadležnosti pojedinih država, posebno ako se imaju u vidu velike različitosti između kaznenopravnih sustava u raznim dijelovima svijeta. Stoga vjerujemo da će u daljnjoj budućnosti ovakva ponašanja sve više potpadati pod nadležnost međunarodnih sudova.

Ovo kazneno djelo u literaturi je još poznato i kao „*Nigerijska prijevara*“, odnosno „*Scam 419*“, nakon što je po prvi put u svijetu normirano u čl. 419. nigerijskoga kaznenog zakona.[10] Nigerijska prijevara sastoji se od toga da počinitelj šalje e-mail oštećeniku u kojem mu lažno obećava određenu imovinsku korist, ako mu oštećenik da broj vlastitog računa ili plati određenu svotu novca. Nakon što dobije tražene podatke, počinitelj prekida sve veze s oštećenikom. Iako se čini bezazlenim, istraživanja pokazuju da na deset tisuća poslanih lažnih e-mailova, barem jedna osoba nasjedne na počiniteljevu prijevaru.[11] Neka istraživanja pokazuju da je, primjerice, u SAD-u u razdoblju od sredine 1980-ih do sredine 2000-ih ovom obliku prijevare podleglo preko 100.000 ljudi, uz imovinsku štetu od preko pola milijarde dolara.[12]

Možemo zaključiti da je takvo postupanje tipičan primjer izravne računalne prijevare. Počinitelj dovodi u zabludu oštećenika koristeći računalni sustav, odnosno e-mail kao sredstvo. Pritom je situacija vrlo specifična jer se počinitelj i oštećenik uopće ne susreću (niti će se ikad susresti) u stvarnom životu, nego se sve odvija u virtualnom svijetu. Ovakvo bi ponašanje u hrvatskom kaznenom pravu, u nedostatku posebne odredbe, valjalo podvesti pod opće kazneno djelo prijevare. Takvo rješenje, međutim, po našem mišljenju otvara jedan važan praktičan problem. Naime, postavlja se pitanje u kojem trenutku počinitelj izlazi iz stadija nekažnjivih pripremnih radnji i ulazi u stadij kažnjivog pokušaja. Je li to već u trenutku kad šalje e-mailove na više različitih adresa ili tek u trenutku kad mu netko od adresata uistinu i odgovori, odnosno pošalje tražene podatke pa on otpočne s daljnjim računalnim operacijama kojima će sebi pribaviti protupravnu imovinsku korist? Prema našem mišljenju, valja se opredijeliti za drugo rješenje. Hrvatski Kazneni zakon u čl. 34. dopušta da se početkom pokušaja smatra i radnja koja «*prostorno i vremenski neposredno prethodi ostvarenju bića*». To znači da između takvih radnji i bića ne smije više stajati neke bitne međuradnje.[13] U ovom slučaju počinitelju predstoji više bitnih međuradnji. Također, smatramo da se u ovako ranom trenutku još ne može govoriti o ispunjenosti pokušajne namjere jer počinitelj, koji je poslao e-mailove na različite adrese, još nema u vidu konkretnog oštećenika. Za oblikovanje potrebne namjere je, po našem mišljenju, nužno da počinitelj zna tko je oštećenik. To će, pak, biti moguće tek onda kada mu oštećenik da potrebne podatke.

10 Hartikainen, E. I., The Nigerian Scam: easy money on the internet, but from whom?, University of Chicago, 2006., str. 1 i dalje.
11 Šepec, M., op. cit., str. 992.
12 Hartikainen, E. I., op. cit., str. 1.
13 Novoselec, P. i Bojanić, I., Opći dio kaznenog prava, Pravni fakultet Sveučilišta u Zagrebu, Zagreb, 2013., str. 299 – 300.

Još jedan vrlo rasprostranjen oblik prijevarnog postupanja uz korištenje računalnog sustava i interneta je i prijevarna kupnja ili prodaja putem interneta. Prijevarna kupnja počinjena je kad počinitelj, nakon što primi stvar, ne uplati traženu svotu novca ili pošalje ček bez pokrića. Prijevarna prodaja počinjena je kad počinitelj, nakon što primi uplatu, uopće ne pošalje traženu stvar ili ju pošalje, ali ona nema tražena svojstva. Nju, također, možemo svrstati u izravne računalne prijevare. Ovo je, prema nekim statistikama, najčešći oblik internetske prijevare.[14] Ovdje se može pojaviti problem dokazivanja potrebne namjere jer se naručena roba transportira poštom iz udaljenih dijelova svijeta pa je uvijek moguće da se izgubi ili ošteti na putu.[15] I za ovu vrstu prijevare vrijedi da se može počiniti s izravnom i s neizravnom namjerom.[16]

Smatramo kako bi, *de lege ferenda*, trebalo razmisliti o uvođenju posebnog oblika prijevare fizičke osobe putem računalnog sustava, bilo u okviru općeg kaznenog djela prijevare, bilo posebnom odredbom. Držimo da se ovaj oblik prijevare ipak značajno razlikuje od klasičnog oblika, prije svega jer se odvija u virtualnom prostoru. Tradicionalno kazneno pravo je, naprotiv, znatno više orijentirano na povredu materijalnih pravnih dobara koja egzistiraju u stvarnom okružju. Ta nematerijalna priroda djela, uz složenost samog računalnog sustava, anonimnost njegovih korisnika i globalnu važnost internetske povezanosti stavljaju kazneno pravo pred nove izazove.[17] Osim toga, smatramo da se izravnom računalnom prijevarom ne povrjeđuje samo imovina i povjerenje oštećenika, kao što je to slučaj kod obične prijevare, nego se ugrožava i normalno funkcioniranje računalne mreže. Važnost interneta u suvremenom životu često se uspoređuje s važnošću vodne mreže ili električne energije.[18] Stoga vjerujemo da ovo djelo zaslužuje izdvajanje u posebnu glavu. U njemačkoj literaturi općenito se preporučuje zakonodavcima da, kada je u pitanju računalni kriminalitet, teže razvijanju novih kaznenih djela ili modificiranju postojećih kako bi izbjegli probleme u tumačenju u sudskoj praksi i pribjegavanje zabranjenoj analogiji.[19]

2.2. Neizravna računalna prijevara i problem zabranjene analogije

Neizravni oblik računalne prijevare sastoji se od toga da počinitelj «manipulira računalnim podacima ili programima s namjerom stjecanja protupravne imovinske

14 Usp. Šepec, M., op. cit., str. 987.
15 Ibid.
16 Tako i Novoselec, P. i Bojanić, I., u Novoselec, P. (ur.), op. cit., str. 239. Valja napomenuti da je hrvatska sudska praksa sklona zastupati stajalište da je prijevaru moguće počiniti samo s izravnom namjerom. Mi se priklanjamo shvaćanju da u obzir dolaze i izravna i neizravna namjera.
17 Tako i Sieber, U. u Sieber/Brüner/Satzger/Heintschel-Heinegg (Hrsg.), op. cit., § 24, r. b. 10 – 11.
18 Ibid., r. b. 8.
19 Usp. npr. Schuhr, J. C., Analogie und Verhaltensnorm im Computerstrafrecht, Am Beispiel der Datenveränderung (§ 303a StGB und Art. $ Convention on Cybercrime), Zeitschrift für Internationale Strafrechtsdogmatik, 8-9/2012, str. 441.

koristi.»[20] Zbog takvih manipulacija računalni sustav više ne može raspoznati pristupa li mu ovlaštena ili neovlaštena osoba.

Ovo kazneno djelo značajno se razlikuje od općega kaznenog djela prijevare jer se ovdje oštećenik ne dovodi u zabludu niti se održava u zabludi.[21] Dok prijevaru redovito karakterizira i određeni doprinos žrtve, uvjetovan njezinom naivnošću ili pohlepnošću,[22] ovdje takvoga doprinosa nema. Već smo napomenuli da se računalni sustav ne može «prevariti» u tradicionalnom kaznenopravnom tumačenju te riječi. Stoga se može postaviti i terminološko pitanje je li ovo djelo uopće prikladno nazivati «prijevarom» ili bi bolje bilo koristiti neki drugi termin poput «zlouporabe».[23]

U zemljama koje ne poznaju posebno kazneno djelo računalne prijevare postoji značajna pravna praznina jer se ovaj oblik ne može podvesti pod opće kazneno djelo prijevare. Takvo bi postupanje očigledno kršilo zabranu analogije. Stoga se u literaturi vrlo često upozorava da je implementacija ovog oblika nužna pretpostavka osuvremenjivanja kaznenog prava.[24] To, uostalom, vrlo jasno zahtijeva i već spomenuti čl. 8. Konvencije.

Kao potpisnica Konvencije, Hrvatska je implementirala kazneno djelo računalne prijevare u vlastiti kaznenopravni sustav. Ovo djelo uvedeno je u hrvatsko kazneno zakonodavstvo još novelom iz 2004. godine, kao čl. 224a u glavi kaznenih djela protiv imovine. Novi je Kazneni zakon, koji je stupio na snagu početkom 2013. godine, uz određene izmjene, preuzeo tu odredbu i premjestio u posebno poglavlje kojim se reguliraju kaznena djela protiv računalnih sustava, programa i podataka. Ovu promjenu treba pohvaliti jer se ovdje ne radi o tipičnom imovinskom deliktu. Novom koncepcijom jasnije se naglašava specifičnost ovog kaznenog djela te njegova važnost za normalno funkcioniranje računalnih sustava i mreža.[25] Ovakvom sistematizacijom svakako je postignuta i bolja preglednost.

Ona se značajno razlikuje od prijašnjeg rješenja. Prema starom Kaznenom zakonu, računalna prijevara bila je regulirana člankom 224.a, u sklopu kaznenih djela protiv imovine. Ta je odredba bila smještena odmah poslije opće odredbe o prijevari (stari čl. 224.). Prema tom rješenju, kazneno djelo računalne prijevare počinila bi osoba kojoj je cilj sebi ili drugome pribaviti protupravnu imovinsku korist tako da unese, koristi, izmijeni, izbriše ili na drugi način učini neuporabljivim računalne podatke ili programe, ili onemogući, ili oteža rad, ili korištenje računalnog sustava ili programa i tako prouzroči štetu drugome. No, osim neizravnog oblika računalne prijevare, tim je člankom također bila regulirana i zlouporaba naprava.

20 Turković, K. i dr., Komentar Kaznenog zakona, Zagreb, 2013., str. 345.
21 Ibid.
22 Usp. Novoselec, P. i Bojanić, I., u Novoselec, P., (ur.), op. cit., str. 234.
23 Ipak treba reći da je termin «*prijevara*» uobičajen i u komparativnom pravu. Tako, primjerice, njemački StGB u § 263a govori o «*Computerbetrug*» (računalna prijevara), a i sama Konvencija rabi termin «*computer fraud*». Stoga našu primjedbu valja shvatiti isključivo u duhu hrvatskoga jezika.
24 Šepec, M., op. cit., str. 992.
25 Tako i Turković, K. i dr., op. cit., str. 341.

To znači da se, prema starom Kaznenom zakonu, nije vršilo jasno zakonsko razlikovanje između neizravne računalne prijevare i zlouporabe naprava, što nije bilo prihvatljivo. Zlouporaba naprava je sadržajno i strukturno različita od računalne prijevare. Zlouporaba naprava sastoji se u neovlaštenom izrađivanju, nabavljanju, prodaji, posjedovanju ili stavljanju drugome na raspolaganje posebnih naprava, sredstava, računalnih podataka ili programa stvorenih ili prilagođenih za činjenje različitih oblika računalnog kriminaliteta. Ovo djelo zapravo predstavlja kažnjivu pripremnu radnju koja može dovesti do neizravne računalne prijevare, ali i do drugih kaznenih djela iz ove domene.[26] Stoga je dobro da je novi KZ to djelo regulirao odvojeno od računalne prijevare.

U novom Kaznenom zakonu neizravna računalna prijevara regulirana je člankom 271.[27] Ta je odredba u potpunosti usklađena sa zahtjevima čl. 8. i 19. Konvencije.[28] Kako je napomenuto, novi Kazneni zakon donosi veliku promjenu kod regulacije računalnog kriminaliteta uvodeći novu glavu o kaznenim djelima protiv računalnih sustava, programa i podataka. Navedena glava regulira osam kaznenih djela, među kojima je i kazneno djelo računalne prijevare koje je regulirano u članku 271. Kaznenim djelom računalne prijevare regulira se neizravni oblik računalne prijevare, dok izravni oblik, kao prema starom Kaznenom zakonu, valja podvesti pod opće kazneno djelo prijevare.

Temeljni oblik ovoga kaznenog djela ostao je u bitnim obilježjima isti. Tako i prema novom Kaznenom zakonu računalnu prijevaru čini onaj tko *s ciljem da sebi ili drugome pribavi protupravnu imovinsku korist unese, izmijeni, izbriše, ošteti, učini neuporabljivim ili nedostupnim računalne podatke ili ometa rad računalnog sustava i na taj način prouzroči štetu drugome* (čl. 271. st. 1.). Smatramo kako «drugi» iz zakonskog opisa može biti i fizička i pravna osoba. Ipak, po naravi stvari, to će najčešće biti pravna osoba – banka u čijem je vlasništvu bankomat ili sl., dok će fizička osoba biti oštećena tek posredno.[29]

U odnosu na regulaciju iz čl. 224a starog KZ-a, nova odredba donosi promjene u drugom i trećem stavku članka 271. Drugi stavak regulira kvalificirani oblik računalne prijevare gdje će se počinitelj teže kazniti, ako je kaznenim djelom računalne prijevare pribavljena znatna imovinska korist ili prouzročena znatna šteta. Prema novom pravnom shvaćanju koje je Kazneni odjel VSRH zauzeo na sjednici od 27. prosinca 2012. (br. Su-IV k-4/2012-57), navedena će obilježja postojati ako korist, odnosno šteta prelaze 60.000,00 kn. To je povećanje u odnosu na prijašnju praksu koja je granicu postavljala na 30.000,00 kn. U trećem stavku istoga članka

26 I njemačka literatura jasno zastupa stajalište da se izrada i pribavljanje opreme za računalni kriminalitet ne može podvesti pod biće računalne prijevare iz § 263a StGB-a. Usp. Seidl, A., Debit Card Fraud: Strafrechtliche Aspekte des sog. «Skimmings», Zeitschrift für Internationale Strafrechtsdogmatik, 8-9/2012, str. 417.

27 Čl. 271. st. 1. KZ: „*Tko s ciljem da sebi ili drugome pribavi protupravnu imovinsku korist unese, izmijeni, izbriše, ošteti, učini neuporabljivim ili nedostupnim računalne podatke ili ometa rad raču-nalnog sustava i na taj način prouzroči štetu drugome*."

28 Usp. Turković, K. i dr., op. cit., str. 345.

29 Šepec, M., op.cit., str. 987.

nalazi se odredba prema kojoj će se podatci koji su nastali počinjenjem kaznenog djela računalne prijevare uništiti, za razliku od regulacije u starom Kaznenom zakonu gdje su se podatci koji su nastali počinjenjem djela oduzimali počinitelju, bez određivanja hoće li se uništiti, sačuvati ili iskoristiti u neke druge svrhe. Kod ovoga djela će, ukoliko je počinjeno putem interneta, doći u obzir i primjena vrlo kontroverzne nove sigurnosne mjere zabrane pristupa internetu iz čl. 75.[30]

Kazneno djelo računalne prijevare kao posebno kazneno djelo neizostavan je dio suvremenog kaznenog zakonodavstva. Oni zakoni koji ne sadrže takvo djelo ostavljaju značajan kaznenopravni prostor nereguliranim, s obzirom na to da se općim kaznenim djelom prijevare mogu pokriti tek izravne računalne prijevare. Zbog toga se u takvim sustavima u praksi često mogu vidjeti slučajevi kršenja zabrane analogije na štetu počinitelja kaznenog djela.

Rečeno možemo prikazati i primjerima iz susjedne Slovenije te iz prijašnje hrvatske sudske prakse. Iako je Slovenija potpisnica Konvencije, slovenski Kazneni zakon još uvijek nije predvidio regulaciju neizravne računalne prijevare. Tu značajnu pravnu prazninu slovenski sudovi pokušavaju pokriti na različite načine. Tako je u slučaju u kojem je počinitelj neovlašteno pristupio računalnom sustavu banke preko bankomata i oštetio banku za određen iznos novca koji je uzeo iz bankomata, Visoki sud u Ljubljani otklonio prijevaru uz obrazloženje da kazneno djelo prijevare može biti počinjeno samo ako je prevarena stvarna osoba, a ne računalni sustav (VSL III Kp 4/2008 od 4. rujna 2008.). Ta je odluka u slovenskoj teoriji ocijenjena kao «apsurdna i posve u suprotnosti s Konvencijom koju je Slovenija ratificirala 2004. godine».[31] U istom je slučaju sud zaključio da se radi o slučaju počinjenja kaznenog djela teške krađe. Prema slovenskom Kaznenom zakonu, za postojanje kaznenog djela teške krađe traži se da počinitelj svladavanjem većih prepreka dođe do stvari iz određenog zatvorenog prostora. U tom smislu, Sud je zauzeo stajalište da je bankomat službeni prostor banke iz kojeg počinitelj uzima određeni dio novca te samim time oštećuje banku za isti iznos novca. Ista situacija pojavljuje se i u odlukama Vrhovnog suda Slovenije I Ips 98/2004 od 31. svibnja 2005. te I Ips 461/2007 od 31. siječnja 2008.[32] Navedeni su slučajevi riješeni tako da su slovenski sudovi određeno činjenično stanje podveli pod one mogućnosti koje su im u tom trenutku bile na raspolaganju u njihovom kaznenom zakonu.

Slična je praksa postojala i u Hrvatskoj prije nego je kazneno djelo računalne prijevare implementirano u hrvatsko kazneno zakonodavstvo. Tako je Županijski sud u Bjelovaru (Kž-397/02 od 7.11.2002.) označio neovlašteno podizanje novca iz bankomata kao kazneno djelo teške krađe. Prethodna krađa kartice, u tom slučaju ulazi u sastav jedinstvenog produljenog kaznenog djela teške krađe.[33] Osim slučajeva

30 Tako Turković, K. i dr., op. cit., str. 345. Za kontroverze oko ove sigurnosne mjere v. Cvitanović, L. i Glavić, I., Uz problematiku sigurnosne mjere zabrane pristupa internetu, Hrvatski ljetopis za kazneno pravo i praksu, 2/2012, str. 914 – 915.

31 Šepec, M., op. cit., str. 993.

32 Ibid., str. 994.

33 Novoselec, P., Podizanje novca na bankomatu pomoću ukradene kartice, Sudska praksa, Hrvatski ljetopis za kazneno pravo i praksu, 2/2008, str. 1167.

neovlaštenog podizanja novca iz bankomata, starija hrvatska kaznenopravna praksa zabilježila je i slučaj uporabe lažne telefonske kartice na telefonskim govornicama. Optuženik je kupio lažnu telefonsku karticu od neutvrđene osobe te je pomoću nje s javne telefonske govornice u Garešnici obavio više telefonskih razgovora. Na isti je način, utrošio, a da nije platio, 53.800 impulsa te oštetio HTP Telekomunikacijski centar Bjelovar u iznosu od 11.082 kune. Općinski sud u Garešnici donio je presudu u kojoj je počinitelj proglašen krivim za kaznena djela krađe i krivotvorenja znakova za vrijednost te mu izrekao uvjetnu osudu. Kako su se obje stranke odrekle prava na žalbu, a nijedna nije zahtijevala dostavu presude, sud je u pisano izrađenoj presudi ispustio obrazloženje (K-9/98-10 od 23.4.1998).[34] Računalna prijevara u to vrijeme bila je relativno nov pojam i nije bila implementirana u hrvatsko kazneno zakonodavstvo. Općinski sud u Garešnici služio se zabranjenom analogijom označivši tu situaciju kao krađu i krivotvorenje znakova za vrijednost. Takva kvalifikacija nije se mogla prihvatiti jer se telefonski impulsi, ni uz najšire moguće tumačenje, tada nisu mogli podvesti pod pojam pokretne stvari.[35] Nedugo kasnije, Kazneni zakon je prijašnju definiciju pokretne stvari proširio i na telefonske impulse. Tek nakon toga se telefoniranje pomoću lažne telefonske kartice moglo razmatrati u okviru, s obzirom na to da kazneno djelo računalne prijevare još nije bilo implementirano u Kazneni zakon. Također, telefonska kartica smatra se običnom ispravom te se uporaba iste smatra kaznenim djelom krivotvorenja isprave, a ne krivotvorenja znakova za vrijednost.[36] No, ovdje valja napomenuti kako nije sasvim sigurno radi li se o neizravnoj ili izravnoj računalnoj prijevari. Naime, telekomunikacijski centar može još za vrijeme telefoniranja utvrditi uporabu lažne kratice te mjesto poziva. Imajući to u vidu, možemo reći kako nam se čini da je ovaj slučaj bliži izravnoj računalnoj prijevari jer počinitelj obmanjuje fizičku osobu koristeći se računalnim sustavom kao sredstvom prijevare. Pošta je glede telefonskih kartica dala uvjetni pristanak, tj. pristala je isporučiti telefonske impulse samo na temelju prave telefonske kartice. Prema tome, korisniku lažne telefonske kartice pošta telefonske impulse ne predaje dobrovoljno i uz poznavanje svih okolnosti slučaja, nego ih on oduzima pošti i time ostvaruje sva obilježja računalne prijevare.[37]

No, još je zanimljiviji slučaj Županijskog suda u Splitu, Kž 205/08 od 20.5.2008. (Općinski sud u Omišu, K124/07) jer je, u trenutku počinjenja djela, kazneno djelo računalne prijevare bilo implementirano u hrvatsko kazneno zakonodavstvo. Optuženik i optuženica počinili su kazneno djelo krađe tako da je optuženica ušla kroz otvorena vrata u jednu obiteljsku kuću u Omišu te iz ženske torbe uzela novčanik u kojem su se nalazili 20 kuna te bankovna kartica s tajnim osobnim brojem (PIN), dok je za to vrijeme optuženik držao stražu. Nakon toga, istog

34 Novoselec, P., Sudska praksa - Materijalno kazneno pravo, Hrvatski ljetopis za kazneno pravo i praksu (Zagreb), vol. 7, broj 1/2000, str. 237.
35 Ibid., str. 238.
36 Ibid.
37 Tako i ibid.

je dana optuženik u četiri navrata na bankomatima u Omišu i Dugom Ratu podigao ukupno 1600 kn, dok je tog puta optuženica čuvala stražu. Općinski sud u Omišu izrekao je prvostupanjsku presudu u kojoj su optuženik i optuženica proglašeni krivima za supočiniteljstvo u kaznenim djelima krađe (kartice) i računalne prijevare. No, povodom podnesenih žalbi drugostupanjski je sud (Županijski sud u Splitu) po službenoj dužnosti preinačio prvostupanjsku presudu te utvrdio da su optuženici počinili kazneno djelo teške krađe. Sud je vlastitu presudu obrazložio tvrdnjom da su okrivljenici uporabom kartice tekućeg računa s pribavljenim PIN brojem za navedenu karticu provalili u zatvoreni prostor, tj. bankomat, uzevši pri tomu novac kako bi ga protupravno prisvojili. To stajalište s pravom kritizira Novoselec. On upozorava da je računalna prijevara u odnosu prema teškoj krađi lex specialis te joj valja dati prednost. Uz to, tim se djelima štite različita pravna dobra. Takvo je rješenje prihvaćeno i u poredbenoj praksi.[38] Možemo se nadovezati primjedbom kako je vrlo dvojbeno ne krši li se podvođenjem računalne prijevare pod tešku krađu zabrana analogije. Naime, kod računalne prijevare nije u pitanju klasični pojam «zatvorenog prostora», nego tzv. «kibernetski zatvoreni prostor». U listopadu 2006. Združeni stožer oružanih snaga SAD-a definirao je kibernetski prostor kao „područje koje karakterizira upotreba elektroničkog i elektromagnetskog dijapazona za pohranjivanje, modificiranje i razmjenjivanje podataka putem mrežnih sustava i povezanih fizičkih infrastruktura".[39] Kibernetski prostor označava virtualni prostor koji nastaje korištenjem računalne i digitalne tehnologije. Taj se prostor ne može podvesti pod definiciju klasičnog prostora koji je obuhvaćen kaznenim djelom krađe ili teške krađe, jer počinitelj ne ulazi izravno u tuđi prostor, nego putem računala zadire u kibernetski prostor. Kibernetski prostor sve je češći oblik ljudske socijalizacije te je njegovo svakodnevno korištenje ključno za čovječanstvo. On se svakodnevno razvija, širi svoje granice i povećava svoj kapacitet. Upravo se stoga povećava i broj kaznenih djela vezanih uz kibernetski prostor, što uključuje i računalnu prijevaru. Takva kaznena djela vrlo se teško otkrivaju, a razlozi tomu jesu: informativni medij koji se ne može izravno očitavati; izmjene i brisanje podataka koji se mogu izvršiti bez ostavljanja ikakvih tragova; zapisi koji ne sadrže pečate i potpise kojima bi se potvrdila njihova autentičnost i koji bi omogućili utvrđivanje razlike između kopije i originala; pristup do podataka i manipuliranje njima može se obavljati s udaljenih terminala; transakcije se obavljaju takvom brzinom koja ne dopušta čovjeku da ih nadzire ni da upravlja njima; programi su smješteni na iste medije kao i podatci, pa se i njima može relativno lako manipulirati; za obavljanje kriminalnih aktivnosti mogu se koristiti vrlo stručne i suptilne metode i tehnike, koje se teško otkrivaju jer ne ometaju redovan rad sustava, a često se mogu dokazati jedino ako se otkriju u trenutku izvršenja.[40] Imajući u vidu posebnosti kibernetskog

38 Ibid.

39 Vuković, H., Kibernetska sigurnost i sustav borbe protiv kibernetskih prijetnji u Republici Hrvatskoj, National security and the future, vol. 13, br. 3, 2012., str. 16.

40 Žužul, J. i Dragičević, D., Informatika u upravi i pravosuđu, Sveučilišna tiskara, Zagreb, 1996., str. 240.

prostora, možemo zaključiti kako podvođenje ovakvih i sličnih ponašanja pod tešku krađu u biti krši zabranu analogije.[41] Uvid u komparativnu praksu pokazuje da su sudovi vrlo skloni posezati za analogijom s drugim kaznenim djelima kada nemaju računalnu prijevaru normiranu u svojim kaznenim zakonima. Tako su, primjerice, u slučajevima u kojima su počinitelji koristili tuđe podatke kako bi putem interneta naručivali robu i plaćanje ostavljali oštećenicima, belgijski sudovi donosili presude za računalno krivotvorenje, dok su finski sudovi osuđivali za povredu tuđe privatnosti.[42] To jasno ukazuje na potrebu postojanja posebnog kaznenog djela računalne prijevare.

3. ZAKLJUČAK

Na prethodnim stranicama obradili smo problematiku računalne prijevare. Pošli smo od shvaćanja da se fenomen računalne prijevare iz kaznenopravnog kuta može promatrati iz uže i šire perspektive. Sukladno tome, predložili smo termine izravna i neizravna računalna prijevara. Pritom je osnovni kriterij razlikovanja bio identitet oštećenika: kod izravne prijevare oštećenik je fizička osoba, a računalni sustav je sredstvo prijevare; kod neizravne prijevare oštećen je sam računalni sustav.

U skladu s tom podjelom, koja koliko nam je poznato još nije bila spominjana u hrvatskoj kaznenopravnoj literaturi, koncipirali smo rad na način da smo prvi dio rada posvetili izravnoj, a drugi neizravnoj računalnoj prijevari. Izravna prijevara se u hrvatskom zakonodavstvu, kao i u većini poredbenih sustava, razmatra u okviru općeg kaznenog djela prijevare. To otvara određene praktične probleme na koje smo u radu upozorili te smo predložili uvođenje zasebnog oblika prijevare pomoću računala, bilo u sastavu općeg dijela prijevare, bilo kao posebnog kaznenog djela. Također smo pokazali i neke od najčešćih oblika izravne prijevare.

U pogledu neizravne prijevare, zauzeli smo stajalište da je normiranje tog kaznenog djela nužno, ne samo da bi se zadovoljili međunarodni standardi, nego i da bi se popunila značajna pravna praznina koja ima sve veću važnost za suvremeno društvo koje ovisi o urednom funkcioniranju računalnih sustava i mreže. U tom smislu, hrvatsko kazneno zakonodavstvo od 2004. pokazuje stalan napredak. Govoreći o neizravnoj računalnoj prijevari, dosta pažnje posvetili smo problemu zabranjene analogije. Taj je problem i inače prisutan kod kaznenih djela računalnog kriminaliteta, a kod neizravne računalne prijevare on poprima dodatnu dimenziju. To smo pokazali na primjerima iz novije hrvatske i poredbene sudske prakse.

41 I Novoselec ističe da je kod računalne prijevare na način opisan u primjerima koje smo naveli zapravo u pitanju «specifično ulaženje u zatvoreni prostor korištenjem računalnih podataka u cilju pribavljanja imovinske koristi». Novoselec, P., Podizanje novca na bankomatu pomoću ukradene kartice, Sudska praksa, Hrvatski ljetopis za kazneno pravo i praksu, 2/2008, str. 1167.

42 Weigend, T., Information society and penal law, General report, XIXth International Congress of Penal Law Preparatory Colloquium, Verona, 2012, Section I – Criminal Law. General Part, str. 56 – 57.

Naš je dojam kako računalnom kriminalitetu u hrvatskoj kaznenopravnoj literaturi i dogmatici još uvijek nije posvećena dovoljna pažnja. U radu smo na više mjesta upozorili na sve veći broj i rastuću pogibeljnost kaznenih djela iz ove skupine. Ova djela stavljaju tradicionalnog kaznenog pravnika pred mnoge izazove kojima često nije u stanju odgovoriti zbog nedostatka informatičkog znanja te zbog nepostojanja adekvatnog zakonodavstva. Računalna prijevara jedno je od takvih djela, koje zbog svoje učestalosti i velike društvene opasnosti zaslužuje posebno mjesto u literaturi. Nadamo se da će ovaj rad potaknuti daljnju raspravu o računalnoj prijevari, ali i o računalnom kriminalitetu u cijelosti.

Summary

COMPUTER- RELATED FRAUD IN CROATIAN CRIMINAL LAW

In this paper, the authors deal with the problem of computer- related fraud. Computer- related fraud, as one of the most common and most dangerous forms of cybercrime in recent years, more and more attracts attention in comparative legal theory and practice. In addition, the Convention on Cybercrime of the Council of Europe demands the parties to implement indirect form of computer- related fraud.

For the first time in Croatian criminal law theory, the authors introduce the terms direct and indirect computer- related fraud, critically analyzing both forms with reference to the Croatian and comparative legislation and practice and give their recommendations for the future.

Key words: *fraud, computer system, cyberspace, aggrieved party, banned analogy, attempt.*

Zusammenfassung

COMPUTERBEZOGENER BETRUG IM KROATISCHEN STRAFRECHT

In dieser Arbeit beschäftigt man sich mit der Problematik des computerbezogenen Betrugs. Der computerbezogene Betrug, als eine der öftesten und gefährlichsten Formen der Internetkriminalität, gewinnt viel Aufmerksamkeit in komparativer Literatur und Praxis in den letzten Jahren. Außerdem fordert die Europaratskonvention über die Cyberkriminalität, dass Vertragsparteien die indirekte Form des computerbezogenen Betrugs implementieren.

Die Begriffe direkter und indirekter computerbezogener Betrug werden zum ersten Mal in die kroatische strafrechtliche Literatur eingeführt. Ebenfalls werden die beiden Formen kritisch analysiert mit Rückblick auf kroatische und komparative Gesetzgebung und Rechtsprechung. Es werden auch Vorschläge für die Zukunft gegeben.

Schlüsselwörter: *Betrug, Computersystem, kibernetisch, Geschädigter, verbotene Analogie, Versuch.*

Riassunto

LA FRODE INFORMATICA NEL DIRITTO PENALE CROATO

Nel presente lavoro gli autori si occupano della questione della frode informatica. La frode informatica costituisce una delle forme di criminalità cibernetica più frequenti e più pericolose, la quale negli ultimi anni registra una crescente attenzione nell'ambito comparatistico e nella prassi. Inoltre, la Convenzione sulla criminalità cibernetica del Consiglio d'Europa esige da parte dei paesi sottoscrittori la previsione della forma indiretta della frode informatica.

Gli autori per la prima volta introducono nella letteratura penale croata nozioni quali frode informatica diretta ed indiretta, analizzando criticamente entrambe le forme nell'ambito della legislazione croata e comparata, come pure la prassi, suggerendo delle soluzioni per il futuro.

Parole chiave: *frode, sistema informatico, cibernetico, danneggiato, divieto di analogia, tentativo.*