PRIMJENJIVOST TRADICIONALNIH KAZNENOPRAVNIH KONCEPATA NA RAČUNALNI KRIMINAL

Doc. dr. sc. Igor Vuletić *

UDK: 343.2:004.3/.4
Prethodno znanstveno priopćenje
Primljeno: listopad 2014.

U radu se raspravlja o primjenjivosti tradicionalnih instituta općeg dijela kaznenog prava na kaznena djela računalnog kriminala. Kontinuirani razvoj i napredak društva za sobom nosi i nove oblike kriminala. Jedan takav oblik je i računalni kriminal. Računalni kriminal usko je vezan uz računalnu tehnologiju i internet. Zbog globalne dostupnosti računalne tehnologije broj žrtava ovih kaznenih djela u konstantnom je porastu. Kako bi učinkovito mogli odgovoriti ovom novom izazovu, kazneni pravnici prisiljeni su educirati se u području informatičke tehnologije i interneta. Na zakonodavnom području nužno je da zakonske odredbe slijede suvremene međunarodne trendove i pružaju dovoljnu pravnu podlogu za borbu protiv ovog oblika kriminala. U tom kontekstu rad preispituje mogu li se klasični instituti općeg dijela, poput načela zakonitosti i zabrane analogije, nečinjenja, kažnjivosti pripremnih radnji i sl., jednostavno i bez dodatne prilagodbe primjenjivati na djela računalnog kriminala ili je u ovom području potrebno osuvremenjivanje. Autor analizira iznesene probleme na primjerima iz hrvatskog i poredbenog zakonodavstva i sudske prakse. Pritom autor daje prijedloge za poboljšanje određenih dijelova kaznenog zakonodavstva de lege ferenda*.*

Ključne riječi: računalni kriminal, pokušaj, nečinjenje, sudioništvo, neizravna namjera, analogija

* Dr. sc. Igor Vuletić, docent Pravnog fakulteta Sveučilišta Josipa Jurja Strossmayera u Osijeku, Stjepana Radića 13, Osijek

1. UVOD

Svakodnevni ubrzani razvoj društva i napredak modernih tehnologija stavlja suvremeno društvo pred mnoge izazove. Ti se izazovi odražavaju i na kazneno pravo. Jedno od područja gdje to posebno dolazi do izražaja je računalni kriminal (engl. *Computer crime*, *cybercrime*). Pod tim pojmom, za potrebe ovog rada, podrazumijevamo sva kaznena djela koja se odnose na računalne podatke. Naime, temeljna karakteristika računalne tehnike jest da se ona sastoji od prijenosa i obrade takvih podataka. Pojam računalnog kriminala je, ujedno, širi od pojma internetskog kriminala – potonji se odnosi samo na ona djela računalnog kriminala koja su počinjena putem interneta.[1]

U kaznenopravnoj literaturi najčešće se ističu četiri osnovna izazova koje računalni kriminal postavlja pred tradicionalno kazneno pravo: traženje jedinstvene definicije, edukacija pravnika u informatici, potencijalni sukob kaznenih vlasti između više država i problemi povezani s virtualnom naravi dokaza.[2] Mi ćemo upozoriti i na, po našem mišljenju, peti važan izazov: potrebu za *redefiniranjem* tradicionalnih instituta općeg dijela i njihovom adaptacijom uvjetima računalnog kriminal. Uvjereni smo da mnogi od tih instituta, u obliku u kojem sada postoje u većini kaznenih zakona, jednostavno nisu primjenjivi na djela koja obilježava ponajprije njihova nematerijalna priroda.

Iako je ova tema vrlo važna zbog rastućeg broja ovakvih kaznenih djela i velike potencijalne opasnosti koje ona u sebi nose, postoji vrlo malo radova u svijetu koji se njome sustavno bave. U hrvatskoj literaturi, pak, taj problem nije uopće do sada obrađen. Stoga je cilj ovog rada popuniti tu veliku prazninu i potaknuti daljnju raspravu. Rad ćemo koncipirati kroz sljedeća poglavlja: najprije ćemo obraditi pitanje kršenja zabrane analogije; zatim ćemo govoriti o odgovornosti za nečinjenje; nakon toga ćemo obraditi kažnjivost pripremnih radnji i pokušaja; na kraju ćemo upozoriti i na određene probleme povezane sa sudioništvom, sankcijama i utvrđivanjem kaznene vlasti.

2. KRŠENJE ZABRANJENE ANALOGIJE

Kad govorimo o analogiji u kontekstu kaznenih djela računalnog kriminala, moramo razlikovati dva osnovna pravna fenomena. S jedne strane, postoji

[1] Za više pojedinosti o temeljnim pojmovima računalnog kriminala usporedi Sieber, U., u: Sieber, U.; Brüner, F.-H.; Satzger, H.; von Heintschel-Heinegg, B. (ur.), *Europäisches Strafrecht*, Nomos, Baden-Baden, 2011., § 24, r. b. 1 – 6.

[2] Usporedi npr. Calderoni, F., *The European framework on cybercrime: striving for an effective implementation*, Crime, Law and Social Change, br. 5, 2010., str. 340 – 341.

analogija na zakonodavnoj razini. O njoj je riječ onda kada zakonodavac stvara nova kaznena djela tako da kao predložak uzme već postojeća (klasična) djela i zatim ih modificira u skladu s potrebama suzbijanja računalnog kriminala. Primjerice, kazneno djelo oštećenja računalnih podataka iz čl. 268. KZ-a nije ništa drugo nego poseban, modificirani oblik kaznenog djela oštećenja tuđe stvari iz čl. 235. Kod oštećenja tuđe stvari objekt kaznenog djela su stvari kao materijalni dijelovi prirode, dok su kod oštećenja računalnih podataka objekt djela podaci kao dio virtualnog svijeta. Korištenje takve zakonodavne tehnike legitimno je pravo zakonodavca i na te se slučajeve ne odnosi zabrana analogije. Dapače, analogija je ovdje poželjna jer je riječ o novoj vrsti kriminala i potrebno je modificirati postojeća kaznena djela. Stoga se u njemačkoj literaturi takva zakonodavna tehnika preporučuje, uz upozorenje da treba poštovati zahtjev za određenošću zakonskih opisa.[3]

Međutim, ovakav oblik analogije nosi u sebi i potencijalnu opasnost. Naime, ponekad zakonodavac na opisani način uvodi ili pooštrava kažnjivost radnji koje uopće nisu kažnjive ili su blaže kažnjive ako su počinjene u stvarnom okruženju. Takvim reguliranjem krši se načelo jednakosti. Primjerice, belgijski Ustavni sud utvrdio je povredu prava na jednakost u belgijskom Kaznenom zakonu, koji je za kazneno djelo uhođenja putem interneta predviđao težu kaznu nego za opće kazneno djelo uhođenja.[4]

U tom kontekstu možemo primijetiti da hrvatski KZ, u već spomenutom čl. 268., za kazneno djelo oštećenja računalnih podataka predviđa kaznu zatvora do tri godine i propisuje kažnjivost pokušaja. S druge strane, za kazneno djelo oštećenja tuđe stvari u čl. 235. propisuje samo kaznu do dvije godine i ne propisuje kažnjivost pokušaja. Ostaje nejasno zašto je zakonodavac procijenio da je oštećenje računalnih podataka pogibeljnije od oštećenja tuđih stvari. Zanimljivo je da je zakonodavac upravo u području računalnog kriminala odlučio na više mjesta iskoristiti mogućnost propisivanja kažnjivosti pokušaja za djela za koja je zapriječena kazna zatvora do tri godine. Upitno je je li takvo proširenje kažnjivosti opravdano kod svih djela iz ove skupine. Primjerice, nije jasno zašto je kod računalnog krivotvorenja iz čl. 270. propisana kažnjivost poku-

[3] Više o tome vidi Schuhr, J. C., *Analogie und Verhaltensnorm im Computerstrafrecht, Am Beispiel der Datenveränderung (§ 303a StGB und Art. 4 Convention on Cybercrime)*, Zeitschrift für Internationale Strafrechtsdogmatik, br. 8-9, 2012., str. 441.

[4] 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. 51, 65 i 66.

šaja, dok zakonodavac tu mogućnost nije iskoristio kod privilegiranog oblika krivotvorenja novca iz čl. 274. st. 2.

S druge strane, postoji i analogija u sudskoj praksi. O njoj je riječ onda kada sud popunjava zakonske praznine tako da stvara nova kaznena djela ili proširuje postojeća na temelju sličnosti s postojećim kaznenim djelima.[5] Takva je analogija strogo zabranjena i predstavlja kršenje načela zakonitosti.

U području računalnog kriminala ovakva je analogija, u nedostatku adekvatnih zakonskih odredbi, relativno česta. Ona se javlja kao posljedica nastojanja sudova da tipično materijalne pojmove kao što su stvar, prostor i sl. protegnu na virtualne uvjete računalnog kriminala. To ćemo ilustrirati na nekoliko primjera iz novije poredbene i domaće sudske prakse.

U Nizozemskoj je Vrhovni sud potvrdio osudu za kazneno djelo teške krađe dvojici počinitelja koji su prisilili jednog dječaka da im prepusti virtualni mač i talisman, koji su u igri imali određenu vrijednost. Počinitelji i dječak bili su sudionici iste internetske igre i nisu se osobno poznavali ni dolazili u kontakt. Dječak je uspio u igri osvojiti mač i talisman, nakon čega su oni doznali njegov identitet te ga prijetnjama (u stvarnom životu) natjerali da im prepusti mač i talisman. U ovom slučaju Vrhovni je sud prihvatio vrlo široku interpretaciju stvari kao obilježja krađe.[6] Po našem mišljenju ovaj slučaj tipičan je primjer kršenja zabrane analogije.

Nadalje, čini se kako nisu rijetki slučajevi u kojima sudovi, u nedostatku posebnog kaznenog djela računalne prijevare, posežu za analogijom s krađom ili teškom krađom. 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 zaključio da je riječ o slučaju počinjenja kaznenog djela teške krađe. Prema slovenskom KZ-u 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. Istovjetne odluke je, u dva navrata, donosio i Vrhovni sud Slovenije.[7]

---

5 Takva se analogija još naziva i *zakonska* analogija. Usporedi Novoselec, P.; Bojanić, I., *Opći dio kaznenog prava*, Pravni fakultet u Zagrebu, Zagreb, 2013., str. 71.

6 Weigend, *op. cit.* u bilj. 4, str. 56.

7 Šepec, M., *Slovenian Criminal Code and Modern Criminal Law Approach to Computer-related fraud*, International Journal of Cyber Criminology, *vol*. 6, br. 2, 2012., str. 994.

Sličan slučaj iz hrvatske sudske prakse pokazuje da praksa često luta u području računalnog kriminala, čak i onda kad ima na raspolaganju adekvatan normativni okvir. Riječ je o odluci Županijskog suda u Splitu, Kž 205/08 od 20. svibnja 2008. (Općinski sud u Omišu, K124/07), koja je već komentirana u hrvatskoj literaturi. Optuženica je ušla kroz otvorena vrata u jednu obiteljsku kuću u Omišu te iz ženske torbe uzela novčanik u kojem se nalazilo 20 kuna te bankovna kartica s tajnim osobnim brojem (PIN), dok je za to vrijeme optuženik držao stražu. Nakon toga, istog je dana optuženik u četiri navrata na bankomatima u Omišu i Dugom Ratu podigao ukupno 1600 kuna, dok je pritom 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. Međutim, u povodu 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-om za navedenu karticu provalili u zatvoreni prostor, tj. bankomat, uzevši pri tomu novac s ciljem da ga protupravno prisvoje. 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 djelima se štite različita pravna dobra. Takvo rješenje je prihvaćeno i u poredbenoj praksi.[8] Možemo dodati kako je u ovakvim slučajevima nedvojbeno riječ o kršenju zabrane analogije i to zato što nije riječ o klasičnom zatvorenom prostoru (u smislu teške krađe), nego o tzv. kibernetskom prostoru. Kibernetski prostor nije stvaran, nego je virtualan i stvoren je računalnom tehnologijom.[9] Sukladno tome, ne može se podvesti pod definiciju iz teške krađe jer počinitelj u njega ne ulazi fizički nego s pomoću računala.

Smatramo da navedeni primjeri jasno upućuju na potrebu stalne adaptacije tradicionalnog kaznenog prava zahtjevima računalnog kriminala. Oni također upozoravaju i na potrebu dodatne edukacije sudaca u području računalnog kriminala. Jedino na taj način može se postići adekvatno tumačenje i izbjeći kršenje zabranjene analogije.

---

[8] Novoselec, P., *Sudska praksa – Materijalno kazneno pravo*, Hrvatski ljetopis za kazneno pravo i praksu, *vol*. 7, br. 1, 2000., str. 237.

[9] Za više pojedinosti o pojmu kibernetskog prostora vidi 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.

3. PROBLEM ODGOVORNOSTI ZA NEČINJENJE

Pitanje odgovornosti za nečinjenje u kontekstu ovih kaznenih djela u praksi se ponajprije javlja u pogledu odgovornosti davatelja usluga informacijskog društva (engl. *internet service-provider*) za kaznena djela počinjena u okviru internetske usluge koju on kontrolira. Prema čl. 2. t. 4. Zakona o elektroničkoj trgovini (Narodne novine, br. 173/2003, 67/2008, 36/2009, 130/2011, 30/2014) davatelj usluga informacijskog društva (dalje u tekstu: davatelj usluga) je pravna osoba koja pruža usluge informacijskog društva. Prema čl. 2. t. 2. istog Zakona usluga informacijskog društva obuhvaća određene usluge putem interneta i elektroničke mreže (npr. internetska prodaja, nuđenje podataka na internetu, reklamiranje putem interneta itd.). Sukladno tome, davatelj usluga ima garantnu dužnost poduzimati nadzorne mjere nad aktivnostima i sadržajima koji se odvijaju u sklopu internetske usluge kojom on ravna. U slučaju propuštanja ili zanemarivanja nadzora pod određenim je pretpostavkama moguća i kaznena odgovornost za nečinjenje.

Ovo pitanje dobilo je na važnosti 1997. godine, kada je sud u Münchenu osudio direktora njemačke tvrtke *ComputerServe GmbH* Felixa Somma na dvije godine zatvora uz primjenu uvjetne osude zbog propuštanja garantne obveze u slučajevima širenja dječje pornografije putem servera za koji je ta tvrtka bila odgovorna. Sud je ustvrdio da su tvrtka i njezin direktor imali spoznaje o pornografskim sadržajima koji se odvijaju na njihovu serveru te su imali tehničke mogućnosti zaustaviti daljnju objavu takvih sadržaja, ali su to propustili učiniti.[10] Ta je odluka izazvala velike kritike u njemačkoj stručnoj javnosti. Upozoravalo se da guši slobodu kretanja podataka na internetu te da praktično onemogućuje normalno funkcioniranje suvremenog internetskog sustava. Iako je u povodu žalbe ta presuda preinačena u oslobađajuću, slučaj je skrenuo pozornost na ovu problematiku i potaknuo mnoge rasprave u njemačkoj kaznenopravnoj literaturi. Počelo se inzistirati na tome da se pretpostavke klasične odgovornosti za nečinjenje ponovno razmotre i prilagode okolnostima računalnog kriminala.[11]

---

[10] Za detalje i kritiku presude vidi Kuner, C., *Judgment of the Munich Court in the "CompuServe case" (Somm case)*; dostupno na: http://www.kuner.com/data/reg/somm.html (24. 8. 2014.).

[11] Usporedi Sieber, U., *Verantwortlichkeit im Internet, Technische Kontrollmöglichkeiten und multimediarechtliche Regelungen*, C. H. Beck`sche Verlagsbuchhandlung, München, 1999., r. b. 431 – 435.

Za odgovornost davatelja usluga za nečinjenje potrebno je dokazati da postoji njegova garantna dužnost. Sporno je u čemu je temelj takve dužnosti. Od svih poznatih temelja garantnih dužnosti u literaturi se raspravlja o dvama koji mogu biti relevantni u ovakvim situacijama. To su dužnost na temelju prethodne opasne radnje i dužnost nadzora nad izvorom opasnosti u vlasti počinitelja. Dužnost na temelju prethodne opasne radnje u pravilu neće biti moguće uspostaviti zato što prethodna opasna radnja mora biti protupravna i mora stvoriti neposrednu opasnost za objekt radnje.[12] Omogućavanje pristupa internetu ili omogućavanje pohrane podataka, naprotiv, nisu protupravne radnje niti se njima stvara neposredna opasnost nastupa posljedice iz bića kaznenog djela. To je stajalište potvrdio i njemački Savezni sud.[13] Nešto je složenija situacija s garantnom dužnošću nadzora nad izvorima opasnosti koji su u vlasti počinitelja. Otvaranje pristupa internetu ne dovodi automatski i do konstituiranja ove garantne obveze, nego se traže i dodatne pretpostavke. Tako se traži da se u javnosti stvorilo povjerenje da će određeni garant kontrolirati određeni izvor opasnosti te da se od njega očekuje izvršavanje radnji zaštite kroz dulje razdoblje. Također je potrebno da je riječ o takvom području u kojem nadzor od strane državnih tijela praktično nije moguće provesti. To će, u pravilu, biti slučaj kod onih oblika internetske komunikacije kod kojih je za pristup određenim podacima potrebna pristupna lozinka. Tada je nadzor od strane države onemogućen pa je razumno očekivati da davatelj usluga spriječi počinjenje kaznenih djela. Ipak će i ta osnova garantne dužnosti u praksi iznimno rijetko doći u obzir i to stoga što će se uvijek tražiti postojanje neposredne opasnosti koja dolazi od samog izvora opasnosti, a ne od strane trećih osoba. Primjerice, vlasnik kuće neće biti kažnjen za nečinjenje ako ne ukloni nacističke grafite sa svoje kuće, a da ih pritom nije napisao on nego treće osobe. Jednako tako, davatelj usluga u pravilu ne bi trebao biti kazneno odgovoran ako treći zlorabe njegov internetski sustav.[14]

Kako je vidljivo, garantnu dužnost davatelja usluga bit će moguće uspostaviti samo iznimno i u vrlo ograničenom opsegu. Ako se takva dužnost ipak uspostavi, tada se traže i daljnje pretpostavke. To su sposobnost za radnju, uzročnost nečinjenja i mogućnost da se od garanta zahtijeva poduzimanje određene radnje. Sposobnost za radnju podrazumijeva da davatelj usluga ima na raspo-

[12] To je slučaj u primjeru mladića koji daje heroin svojoj djevojci, nakon čega ona padne u komu. Usporedi Novoselec, Bojanić, *op. cit.* u bilj. 5, str. 146.

[13] Usporedi Sieber, *op. cit.* u bilj. 11, str. 500.

[14] *Ibid.*, str. 501 – 503.

laganju adekvatne mehanizme pomoću kojih može zaustaviti nezakonite radnje korisnika servera. Uzročnost znači da postoji visok stupanj vjerojatnosti[15] da bi poduzimanje traženih radnji spriječilo nastupanje posljedice. Mogućnost da se od garanta zahtijeva poduzimanje određene radnje pretpostavlja vaganje dvaju pravnih dobara. S jedne strane postoji interes društva za zaštitom od kaznenih djela te zaštita djece i maloljetnika, a s druge zaštita slobode govora i izražavanja mišljenja te zaštita slobodnog protoka informacija putem interneta.[16] U tom smislu relevantan je čl. 15. Direktive 2000/31/EZ Europskog parlamenta i Vijeća od 8. lipnja 2000. o pojedinim pravnim aspektima usluga informatičkog društva na unutarnjem tržištu, posebice elektroničke trgovine. Taj članak propisuje da države članice moraju zabraniti svaku vrstu presretanja ili nadziranja komunikacija svima koji nisu pošiljatelji ili primatelji, osim u slučaju zakonitog ovlaštenja. Time se zapravo uspostavlja jedan oblik isključenja kaznene odgovornosti za davatelje usluga. Ipak je to isključenje ograničeno na dva načina. Prije svega, davatelj usluga ne može se pozivati na isključenje odgovornosti ako njegov doprinos prelazi ono što je minimalno potrebno za funkcioniranje mreže. Ako bi on, pak, inicirao prijenos podataka ili bi na neki način modificirao podatke, tada se više ne bi mogao pozivati na ovaj privilegij. S druge strane, davatelj usluga neće se moći pozvati na isključenje kaznene odgovornosti ni kada je bio pravodobno informiran (od strane državnih tijela ili drugih korisnika mreže) o postojanju nezakonitog sadržaja u svojoj domeni, ali nije poduzeo pravodobne mjere za uklanjanje tog sadržaja.[17]

4. KAŽNJIVOST PRIPREMNIH RADNJI I POKUŠAJA

Kod kaznenih djela računalnog kriminala uobičajeno je propisivati kažnjivost pripremnih radnji u nešto većem obujmu nego što je to slučaj kod većine ostalih kaznenih djela. Razlog za takvu zakonodavnu praksu leži u virtualnom karakteru ovih kaznenih djela, zbog čega su mogući problemi u dokazivanju povrede ili ugrožavanja zaštićenih pravnih dobara. Zato je potrebno kaznenopravnu zaštitu pomaknuti u što raniji stadij.[18] Široko kažnjavanje pripremnih radnji zahtijeva i čl. 6. Konvencije o kibernetičkom kriminalu.

---

[15] U pitanju je vjerojatnost koja graniči sa sigurnošću. Usporedi Novoselec, Bojanić, *op. cit.* u bilj. 5, str. 160.

[16] Za više pojedinosti o ovim pretpostavkama vidi Sieber, *op. cit.* u bilj. 11, str. 503 – 505.

[17] Weigend, *op. cit.* u bilj. 4, str. 62 – 63.

[18] *Ibid.*, str. 60.

Ovakav pristup prihvatio je i hrvatski zakonodavac pa je u čl. 272. predvidio kazneno djelo zlouporabe naprava. Tim kaznenim djelom inkriminiraju se različiti oblici pripremnih radnji poduzetih radi ostvarivanja nekog od ostalih kaznenih djela iz glave protiv računalnih sustava, programa i podataka (Glava XXV).[19] Možemo primijetiti i jednu nelogičnost u pogledu propisane kazne. Naime, u st. 1. koji se odnosi na poduzimanje određenih radnji radi pripremanja kaznenih djela iz čl. 266. – 271. zakonodavac je propisao kaznu zatvora do tri godine. S druge strane, istu je kaznu propisao i za kaznena djela iz čl. 267. – 270. (ometanje rada računalnog sustava; oštećenje računalnih podataka; neovlašteno presretanje računalnih podataka i računalno krivotvorenje), dok je za kazneno djelo iz čl. 266. (neovlašteni pristup) za temeljni oblik propisao kaznu zatvora do jedne godine. Iz tog proizlazi da je zakonodavac u području kažnjavanja izjednačio pripremne radnje i dovršeno kazneno djelo, a u slučaju čl. 266. st. 1. čak i propisao stroži okvir za pripremnu radnju nego za dovršeno djelo! Takvo rješenje je nelogično i pravno neodrživo ako se ima u vidu da su pripremne radnje još uvijek vrlo udaljene od dovršenja kaznenog djela i povrede (ili ugrožavanja) zaštićenog pravnog dobra. Zato bi *de lege ferenda* trebalo preispitati navedene kaznene okvire.

U pogledu kažnjivosti pokušaja već smo napomenuli da je hrvatski zakonodavac na više mjesta propisao kažnjivost pokušaja iako je riječ o kaznenim djelima za koja je zapriječena kazna zatvora u trajanju kraćem od pet godina. Zakonodavac je to učinio kod kaznenih djela neovlaštenog pristupa, ometanja rada računalnog sustava, oštećenja računalnih podataka, neovlaštenog presretanja računalnih podataka te računalnog krivotvorenja. Iz toga se može zaključiti da je zakonodavac ova djela ocijenio kao vrlo opasna i pogibeljna za društvo. Zanimljivo je da zakonodavac nije nigdje predvidio mogućnost djelotvornog kajanja. Smatramo da bi *de lege ferenda* trebalo razmisliti i o uvođenju takve mogućnosti kod ovih kaznenih djela, na način kako je to učinjeno primjerice kod kaznenih djela protiv okoliša (čl. 213.).

S obzirom na virtualni karakter djela računalnog kriminala moguće je da će u nekim slučajevima biti teško razgraničiti početak (kažnjivog) pokušaja od (nekažnjive) pripremne radnje. Mislimo da će to osobito doći do izražaja kod prijevara putem elektroničke pošte koje se provode tako da počinitelj uputi vrlo velik broj elektroničkih poruka različitim i najčešće nasumično odabranim primateljima. U tim e-pismima on od njih traži da mu daju podatke o

[19] Usporedi Turković, K. i dr., *Komentar Kaznenog zakona*, Narodne novine, Zagreb, 2013., str. 346.

svojim bankovnim računima kako bi im mogao isplatiti dobitak od igara na sreću, kako bi im ponudio da daju donaciju u dobrotvorne svrhe i sl. Iako se na prvi pogled čini bezazlenim, istraživanja pokazuju da na deset tisuća poslanih poziva najmanje jedna osoba nasjedne na prijevaru.[20] Kod takvih prijevara čini nam se spornim u kojem trenutku počinitelj izlazi iz stadija nekažnjivih pripremnih radnji i ulazi u stadij kažnjivog pokušaja. Je li to već u trenutku kad šalje elektroničku poštu 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? Po našem mišljenju, valja se opredijeliti za drugo rješenje. Hrvatski KZ 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 smiju više stajati neke bitne međuradnje.[21] 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 elektroničku poštu na mnogo adresa, 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.

5. OSVRT NA PROBLEME SUDIONIŠTVA, SANKCIONIRANJA I ODREĐIVANJA KAZNENE VLASTI

U nastavku ćemo posvetiti pozornost još nekim problemima koji do sada nisu bili u većoj mjeri raspravljani u kaznenopravnoj literaturi, a po našem su mišljenju vrlo važni jer mogu izazvati nedoumice u tumačenju kada su u pitanju ova kaznena djela. Ti problemi se odnose na sudioništvo, sankcioniranje te na otežano određivanje kaznene vlasti država.

5. 1. Sudioništvo

Pitanje sudioništva već smo djelomično dotaknuli kada smo govorili o pretpostavkama odgovornosti davatelja usluga za nečinjenje (vidi pod 3.). Na

[20] Usporedi Hartikainen, E. I., *The Nigerian Scam: easy money on the internet, but from whom?*, 2006., dostupno na: http://www.academia.edu/2375357/The_Nigerian_Scam_easy_money_on_the_Internet_but_for_whom_Michicagoan_2006 (24. 8. 2014.).

[21] Novoselec, Bojanić, *op. cit.* u bilj. 5, str. 299 – 300.

ovom ćemo mjestu samo upozoriti da je, u slučajevima u kojima dolazi u obzir kaznena odgovornost davatelja usluga, potrebno razgraničiti je li riječ o počiniteljstvu nečinjenjem ili pomaganju nečinjenjem. Odluku o tome ne treba temeljiti na kriteriju vlasti nad djelom, kao što je slučaj kod činjenja. Naime, vlast nad djelom ovdje nije prikladno mjerilo jer ona pretpostavlja činjenje kao aktivno sudjelovanje u oblikovanju tijeka zbivanja. Naprotiv, mjerilo treba tražiti u tome postoji li garantna dužnost za sprječavanje posljedice. Ako je odgovor pozitivan, tada treba prihvatiti počiniteljstvo, a u suprotnom pomaganje. U slučaju davatelja usluga riječ je, prema tome, o počiniteljstvu. Daljnje je pitanje je li u pitanju supočiniteljstvo ili paralelno počiniteljstvo. Smatramo da treba prihvatiti stajalište po kojem je riječ o paralelnom počiniteljstvu između osobe koja je postavila nezakonit sadržaj i davatelja usluga koji taj sadržaj nije uklonio jer nedostaje zajednička odluka kao nužna pretpostavka supočiniteljstva. K tome, bilo bi teoretski nedosljedno prosuđivati djelovanje jednog supočinitelja prema kriteriju vlasti nad djelom, a propuštanje drugog prema drugim kriterijima.[22]

U kontekstu sudioništva moguća je i jedna vrlo specifična situacija posrednog počiniteljstva. Ona se može javiti u slučajevima slanja računalnih virusa putem elektroničke pošte, kada je za aktiviranje virusa potrebno da primatelj otvori takvu poštu. U takvim situacijama najčešće će primatelj biti u zabludi o stvarnom sadržaju te neće biti svjestan da svojom radnjom omogućava virusu da uđe u zaštićeni sustav. U takvom slučaju, po našem mišljenju, valjalo bi uzeti da je pošiljatelj virusa posredni počinitelj koji koristi zabludu primatelja. Potonji je samo sredstvo koje se nalazi u zabludi o biću. Ta zabluda u ovakvim slučajevima isključuje njegovu kaznenu odgovornost. Drukčije bi, dakako, bilo ako bi primatelj postupao s izravnom ili neizravnom namjerom. Tada bi bila riječ o supočiniteljstvu.

5. 2. Sankcije

Sankcioniranje računalnog kriminala predstavlja poseban problem. S obzirom na to da je riječ o netipičnim kaznenim djelima za koja je u pravilu potrebno napredno informatičko znanje, tradicionalne sankcije poput kazne zatvora

[22] Za više pojedinosti o problemima supočiniteljstva nečinjenjem vidi Bojanić, I., *Počiniteljstvo kao vlast nad djelom*, Hrvatsko udruženje za kaznene znanosti i praksu i Ministarstvo unutarnjih poslova Republike Hrvatske, Zagreb, 2003., str. 170 – 173.

ili novčane kazne često neće biti adekvatne.[23] Stoga je ovo područje kaznenog prava vrlo podobno za razvoj novih, specifičnih sankcija. Pritom treba voditi računa o načelu razmjernosti i ograničenju kaznenopravne prisile.

U pogledu postojanja specifičnih sankcija za područje računalnog kriminala poredbeni sustavi često predviđaju različite mjere oduzimanja tehničkih naprava ili blokiranja internetskih podataka. Primjerice, u Belgiji sud ima na raspolaganju mjeru kojom može onemogućiti pristup podacima koji predstavljaju kazneno djelo ili su produkt kaznenog djela ili su protivni javnom redu i moralu. U tom smislu sud može narediti davatelju usluga ukidanje određenih internetskih stranica. U francuskom i turskom pravu postoje mjere kojima se određenim osobama može zabraniti korištenje interneta na određeno vrijeme.[24]

Kada smo govorili o kažnjivosti pripremnih radnji, upozorili smo na nelogičnost u propisivanju kaznenih okvira za pojedina djela računalnog kriminala (vidi pod 4.). Na ovom ćemo mjestu spomenuti da je hrvatski Kazneni zakon predvidio u čl. 75. novu sigurnosnu mjeru zabrane pristupa internetu u trajanju od šest mjeseci do dvije godine. Ta mjera će se izreći počinitelju koji je kazneno djelo počinio putem interneta ako postoji opasnost da će zlouporabom interneta ponovno počiniti kazneno djelo (čl. 75. st. 1.). O izricanju ove mjere sud će obavijestiti i regulatorno tijelo nadležno za elektroničke komunikacije koje će, zatim, osigurati provođenje mjere (čl. 75. st. 4.). U obrazloženju ovog članka navodi se kako je mjera uvedena radi onemogućavanja počinitelja da ostvaruju kriminalnu djelatnost putem interneta te da su takve mjere trend u poredbenom zakonodavstvu. Praktična posljedica mjere je u tome da osuđenik neće moći sklopiti ugovor o uslugama interneta, pri čemu će se on i dalje moći koristiti računalom te primati i slati elektroničku poštu putem programa u *offline* obliku.[25] Uz navedeno, kod određenih kaznenih djela (npr. računalnog krivotvorenja iz čl. 270. ili računalne prijevare iz čl. 271.) zakonodavac je predvidio i obvezu suda da odredi uništavanje podataka koji su nastali počinjenjem kaznenog djela.

---

[23] Za istraživanje korelacija između izrečenih kazni i počinjenih kaznenih djela kod kibernetskog kriminala u SAD-u vidi Marcum, C. D.; Higgins, G. E.; Tewksbury, R., *Doing Time for CyberCrime: An Examination of the Correlates of Sentence Lenght in the United States*, International Journal of Cyber Criminology, *vol*. 5, br. 2, 2011., str. 825 – 835.

[24] Vidi Weigend, *op. cit.* u bilj. 4, str. 64.

[25] Turković i dr., *op. cit.* u bilj. 19, str. 110. Za kritiku te mjere vidi Cvitanović, L.; Glavić, I., *Uz problematiku sigurnosne mjere zabrane pristupa internetu*, Hrvatski ljetopis za kazneno pravo i praksu, *vol*. 19., br. 2, 2012., str. 891 – 916.

Valja imati na umu još jednu važnu okolnost kod ovakvih kaznenih djela: mnoga od njih čine maloljetni počinitelji (ili čak djeca!), koji su vješti u služenju računalom i internetom te puno vremena provode za računalom. U takvim slučajevima bit će potrebno prilagoditi sustav maloljetničkih sankcija posebnostima računalnog kriminala.

5. 3. Sukob kaznenih vlasti

Već smo istaknuli kako je jedna od osnovnih značajki računalnog kriminala njegov nematerijalni ili virtualni karakter. Ta činjenica može izazvati probleme oko utvrđivanja kaznene vlasti pojedine države ako se uzme u obzir da posljedice kaznenog djela mogu nastupiti u više država te da je ponekad teško utvrditi iz koje je države počinitelj. Ovaj se problem odražava i na procesnom planu kroz pitanje jurisdikcije.

Iz tih razloga bilo bi dobro kod ovih kaznenih djela izbjegavati tradicionalne kriterije poput državljanstva počinitelja i žrtve ili vezivanja uz teritorij počinjenja. Umjesto toga, smatramo da bi se rješenje moglo tražiti u propisivanju posebnog oblika univerzalne jurisdikcije za najteža djela iz područja računalnog, internetskog i kibernetskog kriminala. Na taj bi se način izbjeglo da počinitelji prođu nekažnjeno. Dakako, prihvaćanje takvog modela pretpostavlja i potrebu harmonizacije zakonodavstava u tom području.

6. ZAKLJUČAK

Na prethodnim stranicama obradili smo problem primjenjivosti klasičnih koncepata općeg dijela kaznenog prava na djela računalnog kriminala. Riječ je o temi koja u hrvatskoj kaznenopravnoj literaturi do sada nije bila obrađivana, dok je u poredbenoj literaturi bila zastupljena samo fragmentarno. Pitanjima iz ovog područja bavili su se uglavnom njemački autori.

Obradili smo probleme povezane s načelom zakonitosti i kršenjem zabranjene analogije, odgovornošću davatelja usluga informacijskog društva za neprava kaznena djela nečinjenjem, kažnjivosti pripremnih radnji i pokušaja, sudioništvom, sankcijama i uspostavljanjem kaznene vlasti. Uz te probleme moguće je govoriti i o mnogim drugima, poput odgovarajućeg definiranja ovih kaznenih djela i usklađivanja pravnih sustava u pogledu njihove regulacije, zatim pitanja razloga isključenja protupravnosti, oblika krivnje, zastare itd. Ta bi izlaganja, međutim, daleko premašila opseg našeg rada. Zato smo se odlučili usredotočiti samo na one institute koje smo smatrali najvažnijima u kontekstu predmetne

teme. Pritom smo prikazali određena rješenja iz poredbenog zakonodavstva i upozorili na neke slučajeve iz poredbene sudske prakse. Također smo kritički komentirali i domaće zakonodavstvo te smo davali prijedloge *de lege ferenda* tamo gdje smo to smatrali svrhovitim. Pojedina pitanja koja smo otvorili, poput razgraničenja pripremnih radnji od pokušaja kod prijevare putem e-pošte, razgraničenja pojedinih oblika sudioništva kod odgovornosti davatelja usluga, posrednog počiniteljstva kod slanja virusa putem e-pisama te potrebe za prilagođavanjem maloljetničkih sankcija nisu do sada uopće bila raspravljana ni u domaćoj ni u stranoj kaznenopravnoj literaturi.

Imajući u vidu složenost i sveobuhvatnost iznesene problematike smatramo da je pitanje redefiniranja tradicionalnih kaznenopravnih koncepata i njihove adaptacije na suvremene uvjete računalnog kriminala podobno da bude predmet posebne i sustavne razrade u okviru neke buduće doktorske disertacije. Stoga se nadamo da će ovaj rad skrenuti pozornost hrvatske kaznenopravne znanosti na problematiku računalnog kriminala i potaknuti bogatu znanstvenu raspravu u bližoj budućnosti.

Summary

Igor Vuletić*

THE APPLICABILITY OF TRADITIONAL CONCEPTS OF SUBSTANTIVE CRIMINAL LAW TO COMPUTER CRIMES

The paper discusses the applicability of traditional concepts of the general part of substantive criminal law to computer crime. With the continuous development of the society come new forms of crime. One such form is computer crime.

Computer crime is closely connected to computer technology and the Internet. The number of victims is increasing. In order to combat this dangerous type of crime lawyers must be educated in the field of computer technology and the Internet.

It is also necessary that legal provisions follow modern trends and provide an adequate legal framework to fight this form of crime. This paper raises the question whether or not such traditional institutes of the general part, such as the principle of legality, omission, preparatory acts etc. can be simply and without any adaptation applied to computer crime. The author analyses these problems on certain examples from Croatian and comparative case-law and gives suggestions for improvement of Croatian legislation de lege ferenda.

Keywords: computer crime, attempt, omission, complicity, indirect intent, analogy

* Igor Vuletić, Ph. D., Assistant Professor, Faculty of Law, Josip Juraj Strossmayer University of Osijek, Stjepana Radića 13, Osijek