

Dr. sc. Davor Derenčinović*

PRIKAZ KOLOKVIJA AIDP-a O KIBERNETIČKOM KRIMINALU (Colloquy on Cyber-Crime) (Atena, 10-13. travnja 2003)

U organizaciji Međunarodnog udruženja za kazneno pravo (AIDP) i grčkog nacionalnog ogranka te međunarodne organizacije u Ateni je od 10. do 13. travnja 2003. održan Međunarodni kolokvij o kibernetičkom kriminalu. Riječ je o iznimno aktualnoj temi koja će biti na rasporedu predstojećeg Svjetskog kongresa AIDP-a tako da je Kolokvij poslužio kao dobra prilika predstavnicima nacionalnih ogranka te međunarodne organizacije da se upoznaju s posljednjim trendovima kompjutorskog kriminala i načinima njegova kaznenopravnog suzbijanja. Nakon pozdravnog govora predsjednika grčkog ogranka AIDP-a profesora Dionysiosa Spinellisa i kratkog uvodnog generalnog izvješća profesora Ulricha Siebera s Pravnog fakulteta Sveučilišta u Münchenu, Henrik W.K. Kaspersen, direktor Instituta za kompjutorsko pravo na Vrije Sveučilištu u Amsterdamu, dao je kraći prikaz proceduralnih mjera predviđenih Konvencijom o kibernetičkom kriminalu Vijeća Europe, dok je Emiliano Viano, profesor na School of Public Affairs, American University, govorio o primjeni načela prostornog važenja kaznenog zakonodavstva u progonu kaznenih djela kompjutorskog kriminala. Nakon kraćih uvodnih izlaganja prvoga je dana svoj referat pod nazivom *International Cooperation in Combating Cyber-Crime and Cyber-Terrorism* prezentirao Donald K. Piragoff, viši savjetnik Odjela za kazneno pravo kanadskog Ministarstva pravosuđa. On je u uvodu naznačio temeljne probleme do kojih dovodi razvoj moderne tehnologije i širenje Interneta kao globalne svjetske mreže. Jedna od karakteristika virtualnog svijeta je u tome da različite osobe, pa i one koje čine različite vrste kaznenih djela, mogu brzo, jednostavno i anonimno komunicirati. Ta njihova komunikacija je transnacionalna, za razliku od sustava kaznenog pravosuđa koje zastaje na državnim granicama, što svakako predstavlja velik problem u suzbijanju različitih vrsta kompjutorskog kriminala. To nameće potrebu usklađivanja nacionalnih zakonodavstava kao temeljne pretpostavke za ostvarivanje učinkovite međunarodne suradnje u suzbijanju te vrste kriminala. U procesu usklađivanja pojavljuju se problemi oko definiranja pojma "kompjutorski kriminal" koji su kroz djelovanje globalnih i regionalnih organizacija u posljednje vrijeme ipak

* Dr. sc. Davor Derenčinović, docent na Katedri za kazneno pravo Pravnog fakulteta Sveučilišta u Zagrebu

djelomično ublaženi (Vijeće Europe, Organizacija za gospodarsku suradnju i razvitak, Međunarodno udruženje za kazneno pravo itd.). Osim o definiciji, nema konsenzusa niti oko sadržaja istražnih tehnika koje su, uz one tradicionalne, nužne u otkrivanju kompjutorskog kriminala i procesuiranju osumnjičenih osoba. Nakon što je određen katalog kaznenih djela kompjutorskog kriminala, sljedeći je problem koji otežava međunarodnu suradnju točno definiranje bića djela iz tog kataloga. Tako, primjerice, zakonodavstva nekih država inkriminiraju svaki neovlašteni pristup računalnom sustavu, dok je u drugima zabranjen samo onaj pristup koji je ostvaren unatoč zaštitnim mjerama.

S obzirom na to da računalni podaci vrlo lako mogu biti izbrisani, zamijenjeni ili im na drugi način može biti izmijenjen sadržaj, potrebno je u nacionalnim zakonodavstvima propisati mjere za njihovu hitnu zaštitu. Stoga je privremena mjera hitne zaštite pohranjenih računalnih podataka propisana čl. 16. Konvencije o kibernetičkom kriminalu Vijeća Europe od krucijalne važnosti kako bi se ti podaci sačuvali i kako bi poslije u postupku mogli biti korišteni kao dokaz. Radi toga Konvencija propisuje obvezu država stranaka da provedu potrebne mjere kako bi zakonski bile u mogućnosti izdati nalog nekoj osobi da zaštiti određene pohranjene računalne podatke sve dok je to nužno, ali najviše 90 dana, kako bi nadležnim tijelima bilo omogućeno da zahtijevaju njihovo otkrivanje. Kako je riječ o privremenoj mjeri koja se poduzima u ranim fazama kaznenog postupka ili čak prije njegova započinjanja kada još nije sasvim jasno o kojem se kaznenom djelu radi, čl. 29. Konvencije predviđa da su države stranke dužne usvojiti zahtjev za provedbu te mjere za sva kaznena djela propisana Konvencijom i da ga ne mogu odbiti s obrazloženjem da ne postoji identitet norme odnosno zahtjev dvostruke kažnjivosti. Taj zahtjev može biti odbijen jedino ako se odnosi na djelo koje stranka primateljica smatra političkim djelom ili djelom povezanim s političkim djelom, ili ako stranka primateljica smatra da će izvršenje zahtjeva vjerojatno ugroziti njezin suverenitet, sigurnost, javni poredak (*ordre public*) ili druge bitne interese. U pogledu ostalih kaznenih djela stranke primateljice imaju pravo odbiti zahtjev za zaštitom u slučajevima kada imaju razloga vjerovati da u trenutku otkrivanja uvjet dvostruke kažnjivosti ne može biti ispunjen. Piragoff je u svom referatu argumentirano podržao rješenje iz čl. 16. Konvencije navodeći da bi striktno pridržavanje zahtjeva dvostruke kažnjivosti i kod primjene privremene mjere zaštite pohranjenih računalnih podataka moglo dovesti do gubitka ključnih dokaza o počinjenom kaznenom djelu. U međunarodnoj suradnji vrlo je važna mogućnost prikupljanja računalnih podataka u realnom vremenu i s tim u vezi davanje ovlasti tijelima kaznenog progona da davateljima usluga (*Interet Service* providerima) izdaju nalog ili da oni prikupe ili snime ili pak da surađuju i pomognu nadležnim tijelima da prikupe i snime podatke o prometu u vezi s određenim komunikacijama na

svojem državnom području prenesenima pomoću računalnog sustava. Međutim, u situacijama u kojima ne postoje davatelji usluga (npr. lokalne područne mreže – LAN), nadležnim tijelima kaznenog progona mora biti pravno omogućeno da sama prikupe podatke u realnom vremenu. Na kraju svog referata, Piragoff se osvrnuo i na mjeru presretanja podataka o sadržaju predviđenu čl. 21. Konvencije te na moguće probleme koji se mogu pojaviti u postupku izručenja osoba osumnjičenih za počinjenje kaznenih djela propisanih Konvencijom.

Khaled Mohey Ahmed, sudac iz Egipta, u svom je referatu pod nazivom *Who does what to children, where, why, and how?* obradio različite pravne i praktične aspekte seksualnih zloporaba djece putem Interneta, a osobito proizvodnju i online distribuciju dječje pornografije. Dječja pornografija smatra se jednim oblikom seksualnog iskorištavanja djece kojim se zadovoljavaju seksualne želje odraslih na štetu emotivnog i tjelesnog razvoja djece. Unatoč razlikama u definiciji, većina međunarodnopravnih dokumenata dječju pornografiju definira kao “prikaz seksualno eksplicitnog ponašanja djece, bez obzira na to je li ono stvarno ili simulirano”. Razvoj Interneta utjecao je na porast ponude i potražnje dječje pornografije koja se krije iza naziva poput: Bambini Sex, Boys International, Incestous Love, Finger and Lolita itd. Khaled je u svom referatu upozorio na problem izražene tamne brojke dječje pornografije na Internetu. Razlog takvom stanju pronalazi u činjenici da se trgovinom djecom koja gotovo redovito podrazumijeva i različite oblike njihova seksualnog iskorištavanja uglavnom bave organizirane kriminalne skupine koje zastrašivanjem i korupcijom utječu na sve one koji bi nadležnim tijelima mogli otkriti njihove aktivnosti. Prema grubim procjenama neprofitne organizacije End Child Prostitution, Child Pornography, and the Traffic in Children for Sexual Purposes (ECPAT) broj djece uključene u različite oblike “industrije seksa” bio je oko 500.000 u Brazilu, 400.000 u Indiji, 600.000 na Tajlandu, 200.000 u Nepal u i 300.000 u Sjevernoj Americi. Prihodi se procjenjuju na oko 23 milijarde američkih dolara godišnje. Jedan od uzroka seksualnog iskorištavanja djece je i siromaštvo i nerazvijenost u nekim dijelovima svijeta. Tako, primjerice, roditelji u Indiji i Nepal u prodaju svoju djecu trgovcima robljem uvjereni kako daju novac u zamjenu za njihovo zapošljavanje u gradovima ili sklapanje braka. Na taj način svake godine u lancima prostitucije završi oko 5.000 do 7.000 nepalskih djevojčica mlađih od deset godina. Razvoj Interneta omogućio je pretežnim korisnicima dječje pornografije, a to su uglavnom dobro situirani muškarci srednjih godina iz Europe i Sjeverne Amerike, da do podataka i sadržaja dječje pornografije dođu lakše no ikad prije. Paralelno s tim razvija se proces inkriminiranja različitih aspekata online dječje pornografije – izrade, distribucije, posjedovanja itd. Unatoč tome što većina država inkriminira većinu navedenih aspekata, Khaled upozorava na države koje su u pogledu nekih aspekata dječje pornografije

(npr. kriminalizacije posjedovanja) još uvijek neodlučne – kao npr. Španjolska. No kako se kod online dječje pornografije radi o aktivnosti koja je transnacionalna, to nameće i potrebu da regulacija odnosno kaznenopravna intervencija bude predviđena i implementirana na transnacionalnoj osnovi, dakle suradnjom između država. U tom pravcu Khaled kao osnovu predlaže UN Konvenciju o pravima djeteta koja u čl. 34. i predviđa obvezu država članica da usvoje univerzalne standarde zaštite djece (osoba mlađih od osamnaest godina života) od svih oblika seksualnog iskorištavanja, osobito prostitucije i pornografije.

Christina Busch s Pravnog fakulteta u Barceloni u svom je referatu pod nazivom *Computer-based Crimes against Intellectual Property* prikazala pravnu zaštitu intelektualnog vlasništva kroz određenje pojma “copyright” i srodnih prava te istaknula u čemu se sastoji kršenje prava intelektualnog vlasništva i koji oblici kršenja toga prava predstavljaju kazneno djelo. Jedan od glavnih problema u vezi sa zaštitom autorskih prava jest prevencija tzv. intelektualnog piratstva koje na međunarodnom tržištu dovodi do godišnjih gubitaka od oko 300 milijardi američkih dolara. To upućuje na činjenicu da je taj oblik kršenja autorskih prava dio organiziranog kriminala koji se koristi modernim tehnologijama i deregulacijom tržišta. Suzbijanje te vrste kriminala vrlo je složeno s aspekta dokazivanja jer su objekti radnje sadržaji koji se ne mogu smatrati pokretnim stvarima. Intelektualnim piratstvom najugroženiji su razni kompjutorski programi. Prema posljednjim izvješćima udio programskog piratstva porastao je od 37% u 2000. godini na 40% u 2001. godini. Najviše je ilegalnih programa proizvedeno i distribuirano u Grčkoj i Španjolskoj u kojima se procjenjuje da se oko polovina svih poduzeća koristi nezakonitim kopijama kompjutorskih programa ili čitavih programskih paketa. Zbog tako zabrinjavajućeg porasta proizvođači se sve više koriste različitim zaštitnim mehanizmima koji onemogućavaju njihovo kopiranje (npr. programi poput *Phenoprotecta*, *SecuRoma* ili *SafeDisca* nakon instalacije originalnog programa zapisuju neke karakteristike računala na kojem je program instaliran pa svaki pokušaj instalacije tog originala na drugo računalo nije moguć jer ga program ne prepoznaje). Fenomenologija kršenja autorskih prava upućuje na potrebu usklađivanja nacionalnih kaznenih zakonodavstava i inkriminiranje postupaka kao što su:

- a) izrada “piratskih” kopija,
- b) javna ponuda odnosno distribucija (uglavnom komercijalna) takvih kopija putem Interneta,
- c) neutralizacija mjera zaštite sadržaja na kojima postoje autorska prava,
- d) javna ponuda odnosno distribucija “oruđa” kojima se neutralizira djelovanje spomenutih zaštitnih mjera.

U raspravi, u kojoj je sudjelovao i autor ovoga prikaza, bilo je govora o problemu utvrđivanja mjesta počinjenja kaznenog djela ako je ono počinjeno

na Interetu, o potrebi pojačane zaštite autorskih prava, o primjenjivosti tradicionalnih instituta općeg dijela kaznenoga prava (poticanje, pomaganje, pokušaj, zabluda) na kaznena djela kompjutorskog kriminala te o izbjegavanju višestrukog kažnjavanja. Zanimljivost i iznimna aktualnost teme kao i izvrsna organizacija Kolokvija svakako su dobra najava Svjetskog kongresa AIDP-a koji će se iduće godine održati u Pekingu.

228. str. prazna