mr Mario Reljanović
Institut za uporedno pravo
Beograd

udk: 343.9.018
primljeno: 15.10.2007.

VISOKOTEHNOLOŠKI KRIMINAL – POJAM, REGULATIVA, ISKUSTVA

Komercijalizacija računarske tehnologije i njena masovna primena u poslovne i privatne svrhe, kao i sve razvijeniji sistemi komunikacije među ljudima, uslovili su pojavu nove vrste nedozvoljenog ponašanja – visokotehnološkog kriminala. Visokotehnološki kriminal ima dosta zajedničkih elemenata s postojećim oblicima kriminalnog ponašanja, ali poseduje i specifične elemente, na koje se pokušava ukazati u ovom radu. Osim toga, lišen namere da ponudi definitivne i konačne odgovore, autor ukazuje i na najznačajnije probleme u uporednoj praksi, kao i moguće pravce njihovog rešavanja. Konačno, analiza najvažnijih međunarodnih dokumenata i nacionalnih zakonodavstava pojedinih zemalja otkriva kakve se promene mogu očekivati u ovoj oblasti narednih godina. Analize i iskustva koja su sakupljena na ovaj način, mogu se koristiti kao putokaz daljeg delanja na polju visokotehnološkog kriminala u Srbiji.

1. GLOBALNA DIMENZIJA VISOKOTEHNOLOŠKOG KRIMINALA

Pojava modernih računara i korisničkih programa za najširu upotrebu promenila je živote ljudi širom sveta. Računari se koriste ne samo zarad ubrzavanja osnovnih kancelarijskih poslova, već i za složena projektovanja, baze podataka, komunikaciju, informisanje, edukaciju i zabavu. Sa ovakvim razvojem računara razvile su se i računarske mreže (ili računarski sistemi), od kojih je najpoznatija svetska mreža – internet. Ovakav progres pratilo je i razvijanje ideje o korišćenju novih tehnologija u protivpravne svrhe.

Prvi računari bili su „samodovoljni", izolovani od uticaja ostalih računara. Međutim, računarske mreže su osmišljene ubrzo nakon početka masovnije proizvodnje računara, pre svega da bi se podaci koji se nalaze na različitim računarima mogli deliti (eng. *share*) i distribuirati pojedinim ili svim korisnicima određene mreže. Danas se primeri ovakvih mreža mogu naći u svakoj kompaniji čiji službenici koriste računare u svom poslu, umrežene u jedinstveni sistem radi lakše i brže komunikacije. Takav sistem je dvostruko ranjiv – i spolja i iznutra. Istovremeno, način na koji računari i računarske mreže funkcionišu postali su

zahvaljujući korisničkim programima daleko jednostavniji i pristupačniji većem broju ljudi, koji s minimalnom obukom mogu savladati osnove rada na računaru. Tu činjenicu počeli su da koriste pojedinci koji su, koristeći nepažnju i neiskustvo drugih, obezbeđivali sebi neku vrstu koristi.

S druge strane, sagledati razvoj računara a ne primetiti razvoj ostalih visokih tehnologija ne bi bilo celishodno za razumevanje ove nove vrste društvene opasnosti. Mobilni telefoni, PDA uređaji – svake godine nastupi poneka minirevolucija u inoviranju načina na koji mnogobrojni izumi osmišljeni za prenos informacija, komunikaciju i zabavu funkcionišu, poprimajući neke funkcije koje su do sada bile vezivane isključivo za računare. Ove inovacije, koliko god bile pozitivne, imaju i svoju lošu stranu – prosečan korisnik nema dovoljno volje, niti vremena da se upozna sa opasnostima koje nosi korišćenje ovih uređaja, na taj način označavajući sebe kao „lak plen" iskusnih i daleko bolje edukovanih pojedinaca s nečasnim namerama. Visokotehnološki kriminal je tako postao svakodnevica, a fantastičan razvoj tehnologija je uslovio i neverovatnu diferencijaciju vrsta nedozvoljenih dela koja se mogu izvršiti njihovim korišćenjem, od onih naivnih i bezopasnih koja se uglavnom vezuju za reklamiranje različitih proizvoda, do veoma opasnih ponašanja koja spadaju u teška (ponekad čak i najteža) krivična dela u mnogim nacionalnim zakonodavstvima.

Kako je sve počelo? Prve računarske mreže nastale su u SAD i bile su korišćene u vojne svrhe ili za potrebe vladinih institucija. Nepotrebno je reći da su u takvim uslovima i s obzirom na svoju namenu bile podvrgnute jakoj zaštiti, pa je bilo praktično nemoguće zloupotrebiti ih na bilo koji način. Međutim, civilne mreže koje su nastale na ovaj način ubrzo su ustupile svoje mesto internetu, koji je postao dostupan svima – najpre samo formalno, zbog cene potrebne tehnologije i priključka, a ubrzo i faktički, s obzirom da je nova tehnologija naglo komercijalizovana. U nekim procenama se navodi da je već 1992. godine u SAD bilo oko milion korisnika. U 2000. godini, u svakom trenutku na internetu je bilo oko 50 000 000 ljudi, a ovaj broj se povećava geometrijskom progresijom, budući da neke od najmnogoljudnijih zemalja sveta (Kina, Indija, ceo azijski region) u poslednjoj deceniji vrše ubrzano računarsko „opismenjavanje" stanovništva i čini internet dostupnim i za manje imućne slojeve građana. Posledica ovakve ekspanzije bilo je rađanje globalnog *cybercrime*, krivičnih dela koja su povezana s računarskim tehnologijama. Godine 1998. dogodio se prvi masovni napad na internetu, kada je u mrežu ubačen samoreplicirajući program koji uništava podatke na računarima i širi se samostalno po mreži (eng. *worm* – „crv"). On je napravio veliku štetu i praktično uništio gotovo trećinu internet sadržaja u SAD. To je bio samo početak. Narednih godina gotovo da nije bilo internet prezentacije važnije vladine institucije u SAD, multinacionalne korporacije, međunarodne organizacije i sl. koji nije „hakovan" (eng. *hacked*) – čiji sadržaj nije izbrisan, zamenjen nekim drugim sadržajem, ili sklonjen na izvesno vreme sa interneta, tako što bi neka osoba (osobe) neovlašćeno pristupile računaru-serveru, na kome se čuvaju podaci tih

sajtova.[1] Uporedo s ovim, ponekad čak i simpatičnim i naivnim pokušajima da se skrene pažnja na određeni problem ili da se izrazi protest zbog postupanja neke države ili organizacije, nastale su i prve ozbiljnije finansijske prevare, naročito nakon pojave elektronskog bankarstva polovinom devedesetih godina prošlog veka i korišćenja platnih kartica putem interneta. Na taj način, stvorene su pretpostavke za rađanje modernog visokotehnološkog kriminala.[2]

Međutim, šta tačno podrazumeva visokotehnološki kriminal ili *cybercrime*, kako je originalni naziv ove vrste kriminala koji se odomaćio u mnogim svetskim jezicima? Jedinstveni odgovor na ovo pitanje ne postoji. Osnovna nedoslednost u njegovoj primeni može se obuhvatiti različitim shvatanjem „savremenih tehnologija". Dok je u engleskom jeziku „cyber" (skraćeno od *cybernetics*) prefiks uz izraze koji označavaju računarske ili druge elektronske uređaje ili tehnologije, čime se zapravo predefiniše pojam koji se pod „sajber-kriminalom" može podrazumevati, izraz „hi-tech" (eng. *high technologies*, visoke tehnologije), koji se ranije koristio, uticao je na zakonodavstva pojedinih zemalja koja i dalje ovu grupu krivičnih dela svrstavaju u „visokotehnološki kriminal".[3] Zabuna, međutim, dolazi zato što se ovi pojmovi u praksi (kao i u nacionalnim zakonodavstvima i međunarodnim dokumentima) izjednačavaju, iako to ne bi trebalo činiti. Tako se dolazi do situacije da izjednačeni pojmovi imaju potpuno drugačiju sadržinu: „sajber-kriminal" je ograničen samo na krivična dela koja se vrše (zlo)upotrebom računara i računarskih sistema, a „visokotehnološki kriminal" se ne ograničava samo na računare, već podrazumeva upotrebu bilo koje visoke tehnologije, koja uključuje sva savremena tehnička sredstva. Još veća zabuna nastaje u drugom slučaju, koji nije stran mnogim zemljama, pa ni srpskom zakonodavstvu: visokotehnološki kriminal se izjednačava (i ograničava) sa sajber-kriminalom, tako da ostala moguća krivična dela bivaju potisnuta u drugi plan i izostavljena iz nacionalnih krivičnih zakona. Nepotrebno je reći da su i jedna i druga pojava štetne za suzbijanje ove vrste kriminala, tako da se značajan napor pridaje definisanju sajber-kriminala, dok se ostale vrste visokotehnološkog kriminala

1 Godine 2003. pušten je do sada najdestruktivniji „crv" do sada, „Safirni crv", koji je u roku od deset minuta zarazio 90% računarskih sistema na planeti koji nisu imali (adekvatnu) zaštitu. David Perry, direktor sektora za obrazovanje kompanije *Trend Micro* koja se bavi bezbednošću računara, ističe da napadi na računarske mreže postaju sve sofisticiraniji i teži za uočavanje i odbranu, ali i sve više okrenuti lukrativnoj dimenziji ove aktivnosti. Izvor: Michael Coren, *Cyber-crime bigger threat then cyber-terror*, CNN International, 24.01.2005. (http://www.cnn.com/2005/TECH/internet/01/18/cyber.security, 03.10.2007)

2 Koliko je „moderni" visokotehnološki kriminal opasan može se videti iz napada koji se desio u februaru 2007. godine, kada su „hakeri" simultano napali – sa ciljem potpunog onesposobljavanja – šest od trinaest tzv. „root servera" na internetu. Da su uspeli u svojoj nameri, internet bi kao takav u potpunosti prestao da funkcioniše. Na sreću, samo su dva servera pretrpela značajnije posledice. (Izvor: http://www.crime-research.org/articles/threat-ti-internet, 03.10.2007). Zanimljivu priču o „tradicionalnom" visokotehnološkom kriminalu videti na internet adresi: http://cybercrime.planetindia.net/intro.htm, 03.10.2007.

3 Ipak, pod ogromnim uticajem upotrebe u SAD, izraz „cybercrime" danas ubedljivo prevladava.

uglavnom svrstavaju u posebne oblike izvršenja drugih krivičnih dela, što ona po svojoj prirodi i jesu.[4] Ili, rečima tvoraca *Symantec* korporacije: „Pitate šta je *cybercrime*? Najjednostavniji odgovor je – to je komplikovano!"[5]

Među mnogobrojnim definicijama ovih pojmova, lako je uočiti zajedničke elemente – korišćenje računara ili računarske mreže. Mnoge od njih visokotehnološki kriminal shvataju veoma usko – na primer, jedna od najobuhvatnijih internet enciklopedija tehničkih termina *cybercrime* definiše kao „kriminalnu aktivnost počinjenu korišćenjem računara i interneta".[6] Naravno, u praksi se može dogoditi da počinilac koristi mnogo drugih sredstava za izvršenje krivičnog dela, pa je očigledno da ovako uska definicija ne zadovoljava potrebe za percipiranjem ove vrste kriminaliteta, koje je od neobično velike važnosti za njihovo dalje suzbijanje. Identifikovati šta predstavlja krivično delo visokotehnološkog kriminala i kako se ono razlikuje od drugih vrsta nepoželjnog ponašanja koje nije uvek društveno opasno, osnovni je problem koji nijedna definicija još nije uspela da prevaziđe. Ipak, najveći broj napora da se ovaj problem odredi jednostavno a precizno, završava se definisanjem pojma *cybercrime* kao „vršenje krivičnih dela upotrebom računara ili računarskih mreža".[7] Iako naizgled i suviše jednostavna, ova definicija veoma dobro pokriva široko polje mogućeg kriminalnog delovanja. Ako se izostavi zamerka koncepcijske prirode koja je već iznesena, a koja se odnosi na činjenicu da nisu samo računari moguća oruđa zloupotrebe novih tehnologija, ovakvo određenje se uklapa u rešavanje još jednog problema koji je veoma izražen – svakodnevno uvećavanje liste mogućih kriminalnih ponašanja vezanih za računarske mreže, pre svega (ali ne isključivo) za internet. Ostala dela se moraju inkriminisati u okviru postojećih krivičnih dela, kao njihovi specifični oblici. Pri tome se mora voditi računa o činjenici da savremene tehnologije napreduju daleko brže od mogućnosti zakonodavca da vrši izmene krivičnog prava, kao i o činjenici da u mnogim od ovih oblasti ne postoje utvrđeni međunarodni standardi, niti nedvosmislena praksa. Ovi problemi biće detaljnije razmatrani u nastavku teksta.

---

4 Na primer, velika pažnja se poklanja suzbijanju širenja rasne, nacionalne, verske i drugih oblika mržnje, netrpeljivosti i diskriminacije putem računarskih mreža (pre svega interneta, odnosno različitih internet sajtova). Ovo delo se, međutim, veoma lako može izvršiti i putem mobilnog telefona, slanjem propagandnih poruka (koje su komercijalne i uobičajene za sve operatere širom sveta) diskriminatorske sadržine.

5 Symantec korporacija je jedna od najznačajnijih kompanija na svetu koje se bave bezbednošću računara na internetu. Izvor: http://www.symantec.com/avcenter/cybercrime/index_page2.html, 03.10.2007

6 Izvor: http://www.techterms.com/definition/cybercrime, 03.10.2007. Zanimljivo je da ovo shvatanje nije usamljeno u svetu istraživanja visokotehnološkog kriminala. Pogledati: http://www.crime-research.org/analytics/702, kao i različite enciklopedije i rečnike na internetu, koji prihvataju stanovište o najužem mogućem posmatranju visokotehnološkog kriminala: http://www.thefreedictionary.com/cybercrime, http://www.webopedia.com/TERM/C/cyber_crime.html, http://www.pcmag.com/encyclopedia_term/ 0,2542,t=cybercrime&i=40628,00.asp, 03.10.2007

7 Izvor: http://www.webopedia.com/TERM/C/cyber_crime.html, 03.10.2007

2. VRSTE KRIVIČNIH DELA KOJA SPADAJU U VISOKOTEHNOLOŠKI KRIMINAL

Već je rečeno da je život daleko ispred mogućnosti zakonodavca da inkriminiše sve potencijalno opasne društvene pojave koje su vezane za savremene tehnologije. Zaista, broj dela koja se mogu podvesti čak i pod najrestriktivnije i najuže definicije pojma *cybercrime* se gotovo svakodnevno uvećava. Samim tim je i klasifikacija takvih ponašanja teška, zato što se ne mogu utvrditi kriterijumi koji će određena dela svrstati isključivo u jednu kategoriju, dok pojave novih načina zloupotrebe nužno iziskuju i proširenje pomenute liste kriterijuma. Pavan Dugal, predsednik međunarodne organizacije koja se bavi izučavanjem visokotehnološkog kriminala *Cyberlaws*, izneo je podelu koja zadovoljava osnovne pretpostavka analize, ali ne predstavlja detaljnu klasifikaciju. Dugal deli sva krivična dela iz ove grupe na: dela protiv ličnosti, dela protiv imovine i dela protiv države.[8] *McConnel International* je, u izveštaju o zakonodavstvima pedeset dve zemlje koje su analizirane, sva krivična dela visokotehnološkog kriminala podelio na četiri kategorije: dela povezana s podacima, dela povezana s računarskim mrežama, dela povezana s neovlašćenim pristupom računarima i ostala dela koja imaju elemente ove grupe.[9]

Iako klasifikacija ima veliki značaj pri izučavanju ovih dela, smatramo da nije svrsishodno po svaku cenu praviti veštačke podele. Koliko god kategorija visokotehnoloških krivičnih dela iznašli, uvek će neko izmaći upotrebljenoj logici i ostati po strani napravljenih podela.[10] Zato je praktičniji, iako zasigurno

8 Izvor: http://www.crime-research.org/analytics/702, 03.10.2007

9 Izvor: http://wwwmcconnelinternational.com, 03.10.2007; *McConnel International* je konsultantska firma koja se bavi istraživanjem globalnog tržišta u različitim oblastima, uključujući i savremene tehnologije. S obzirom na to da je izveštaj nastao 2000. godine, ova podela ne uključuje sva dela koja su danas poznata, ali sam tekst njihove analize može lako predočiti u kakvom je razvoju visokotehnološki kriminal, odnosno koliko reakcija država zaostaje za tim razvojem: te godine je od 52 države koje su analizirane (među kojima je bila i Jugoslavija) samo devet imalo potpuno razvijeno zakonodavstvu u pogledu suzbijanja *sajber-kriminala.* Od tih devet zemalja, samo su Filipini uveli inkriminaciju svih tada poznatih oblika krivičnih dela, dok su ostale države po pravilu izostavljale neka koja su, prema tadašnjem shvatanju, spadala u posebne načine izvršenja tradicionalnih krivičnih dela, kao i neka za koja se nije smatralo da nose naročitu opasnost po pojedince ili društvo u celini (internet prevare, presretanje podataka, sabotaža računarskh mreža, falsifikovanje na računarima, diseminacija računarskih virusa i sl).

10 Adam Graycar, direktor Kriminološkog instituta Australije, pokušao je da prevaziđe ovaj problem navođenjem devet kategorija *sajber-kriminala*: dela protiv telekomunikacionih službi, komunikacija u cilju zločinačkog udruživanja, telekomunikaciona piraterija, rasturanje materijala „neprikladnog" sadržaja, pranje novca i evazija poreza, elektronski vandalizam, terorizam i iznuda, prevare u vezi s prodajom i investicijama, nezakonito presretanje telekomunikacija i prevare vezane za elektronsko poslovanje. Širokim definicijama navedenih grupa on je gotovo uspeo da pokrije sve oblike neželjenog i nezakonitog ponašanja. Ipak, koliko je ovaj posao samo relativno koristan i koliko su ovakve podele ponekad neupotrebljive pokazuje analiza „rasturanja materijala neprikladnog sadržaja" – u ovu grupu bi spadale reklamne poruke (čije slanje nije kažnjivo), kao i slanje npr. rasističkih poruka, pornografskog materijala (uključujući i dečiju pornografiju) i uputstava za pravljenje eksplozivnih naprava (dakle, postupci koji se smatraju teškim krivičnim delima u tradicionalnom krivičnom pravu). Izvor: http://www.aic.gov.au/conferences/other/graycar_adam/2000-02-cybercrime.html, 03.10.2007

nepregledniji, pristup koji ćemo primeniti – klasifikacija na osnovu samo nekih zajedničkih karakteristika, bez isključivosti pripadanja samo jednoj od niženavedenih grupa. Priroda ovih dela je kompleksna, pa se tako prema njima treba i postaviti, ističući pre svega kriterijum sveobuhvatnosti i pragmatičnosti. U tom smislu, može se govoriti o sledećim grupama krivičnih dela visokotehnološkog kriminala:

1) Krivična dela protiv računara i računarskih sistema u užem smislu

Predstavljaju najširu grupu dela, koja se konstantno umnožavaju zahvaljujući maštи počinilaca ali i stalnom usložnjavanju i izmenama računara, njihovih karakteristika, funkcija, potencijala, načina povezivanja i sl. Konvencija o visokotehnološkom kriminalu Saveta Evrope[11] ovu grupu naziva „Krivična dela protiv poverljivosti, integriteta i dostupnosti računarskih podataka i sistema", i u nju svrstava sledeća dela:

- *Nelegalni pristup* informacijama sadržanim na računaru ili računarskom sistemu, u nameri da se te informacije prisvoje, izmene ili unište. Za ovo delo se traži *namera*, tako da je državama-potpisnicama ostavljena mogućnost da inkriminišu samo posebne radnje koje dovode do ilegalnog pristupa nekom računaru ili mreži. Tipičan primer ovakvog dela je postavljanje „trojanaca" u nečiji računar. „Trojanci" (eng. *trojans*) se ispoljavaju najpre kao forma nenasilnog preuzimanja kontrole nad tuđim računarom, čega vlasnik računara najčešće nije svestan. „Trojanac" ne može sam da se aktivira, već to *čini korisnik računara koji je napadnut* u ubeđenju da instalira autorizovan program, ili neku drugu aplikaciju za rad na računaru (otud analogija s trojanskim konjem).[12] Slično „trojancima" deluju i „logičke bombe", štetni programi poput virusa, ali bez mogućnosti samostalnog izvršavanja, sve dok ne dobiju komandu od korisnika napadnutog računara koja se najčešće ogleda u pokretanju određenog programa.
- *Nelegalno presretanje* privatnih podataka koji se prenose na bilo koji način između dva računara (ili mreže). Konvencija ostavlja mogućnost državama da ovako definisano delo ograniče postojanjem namere. Kao i u prethodnom slučaju, ova činjenica je bitna pre svega zbog mogućnosti da neko bez svog znanja, ili bar bez ikakve namere, dođe u posed tuđih podataka na računarskoj mreži.
- *Izmena podataka* na računaru, u smislu namernog potpunog ili delimičnog oštećenja, brisanja, promene sadržine, kompresije i bilo kog drugog načina

11 Konvencija je usvojena 2001. godine. Do sada je potpisalo 47 zemalja (od država koje nisu članice Saveta Evrope potpisale su Kanada, Japan, Južna Afrika i SAD), ali su je ratifikovale samo 22, uključujući SAD kao jedinu vanevropsku državu (stanje na dan 03.10.2007. godine). 2003. godine je donet Dodatni protokol uz Konvenciju, koji se bavi inkriminisanjem akata rasističke i ksenofobične prirode počinjenih putem računarskih sistema.

12 Više o „trojancima" na internet stranici: http://en.wikipedia.org/wiki/Trojan_horse_(computing), 03.10.2007

izmene originalnih podataka. Ovo delo možda na prvi pogled izgleda slično *nelegalnom pristupu*, ali se mora shvatiti pre svega kao njemu komplementarno: nelegalni pristup (u nameri da se izmene podaci) omogućava izvršenje samog dela izmene podataka. I ovde Konvencija ostavlja mogućnost sužavanja dometa inkriminacije – države mogu izmenu podataka smatrati krivičnim delom samo ako je pričinjena veća šteta. Postupci opisani u delu nelegalnog pristupa, kao što su „trojanci" i „logičke bombe", zapravo za krajnji cilj imaju izmenu podataka na računaru, ili njihovo slanje autoru štetnog programa (radi dalje zloupotrebe, najčešće preuzimanja identiteta napadnutog računara).

- Na delo izmene podataka nadovezuje se *upad u računarsku mrežu*, koji je na potpuno isti način definisan, ali se odnosi na sistem računara čiji se rad onemogućava ili menja nelegalnim pristupom i izmenom podataka na mreži. Ovo delo se sreće u mnogim nacionalnim zakonodavstvima kao *„uskraćivanje usluga"* (misli se na usluge odgovarajuće računarske mreže zbog nelegalnog upada u njene podatke).
- *Zloupotreba uređaja* je specifično delo koje veoma dobro oslikava s kakvim se problemima mogu nacionalni zakonodavci ili međunarodna zajednica susresti u pokušajima da definišu sva dela visokotehnološkog kriminala. Zloupotreba uređaja je složeno krivično delo, koje pokušava da pomiri načelo *nulla crimen, nulla poena, sine lege* i „bujanje" najrazličitijih krivičnih dela koja su vezana za savremene tehnologije. Zato generalnom odredbom države-potpisnice preuzimaju na sebe obavezu da kazne svaku namernu ilegalnu proizvodnju, posedovanje, upotrebu ili nabavku, prodaju kao i svaki drugi oblik distribucije i činjenja dostupnim nekome ko na to inače nema prava bilo kog „uređaja", pod kojim se podrazumevaju i računarski programi, kao i bilo koji oblik podataka pomoću kojih se mogu izvršiti krivična dela navedena u prethodnim članovima Konvencije. Imajući u vidu revolucionarnost, a verovatno i neodređenost ove odredbe, pisci Konvencije ipak dopuštaju državama da stave rezervu na ovaj član, osim kada je reč o prodaji ili drugom obliku distribucije lozinki ili drugih računarskih podataka pomoću kojih se mogu počiniti navedena dela. Na ovaj način se „uređaji" možda i nepravedno stavljaju u drugi plan, ali se i državama ostavlja da same odrede domašaj pomenutog principa da nema kažnjavanja bez (jasno) inkriminisanog krivičnog dela.

Ovakav pokušaj Saveta Evrope je u skladu s rastućom opasnošću od visokotehnološkog kriminala, a istovremeno zadovoljava i kriterijume koje smo naveli – na generički način sažeti veliku grupu protivpravnih radnji u nekoliko složenih krivičnih dela, čije su inkriminacije dovoljno precizne da mogu poslužiti nacionalnim zakonopiscima, a istovremeno ostavljaju dovoljno slobode budućoj praksi da odredi granice njihovog domašaja bez stvaranja pravne nesigurnosti. To se možda ne može primeniti i na pojam „uređaja", ali je više nego jasno da se u ovom slučaju radi o maštovitom pristupu sa ciljem da se pravo približi realnosti i da se na neki način premosti očigledna razlika između dinamike razvoja pravnih akata i tehničko-tehnoloških mogućnosti za njihovo kršenje, koja sada postoji.

2) Krivična dela protiv autorskih i srodnih prava

Povrede autorskih i srodnih prava nisu novina i njihova pojava se ne vezuje za pojavu računarskih medija i komunikacija. Međutim, razvoj tehnologije u poslednjih nekoliko decenija omogućio je stvaranja novih načina za njihovo izvršenje. Računarski programi, filmovi, muzika, ali i knjige, umetničke fotografije i slično, predmet su konstantne razmene između računara i računarskih mreža. Mali broj ovih razmena je legalan, odnosno predstavlja savremeni oblik kupoprodaje. Razvoj interneta omogućio je da se različite ljudske tvorevine zaštićene autorskim pravima prenesu s jednog kraja sveta na drugi (odnosno s jednog računara na drugi) veoma brzo, ponekad u intervalu od samo nekoliko minuta. Razvoj drugih tehnologija omogućio je prebacivanje ovih sadržaja na pogodne medije (CD, DVD diskovi, flash memorije i sl.) i njihovo neograničeno kopiranje i distribuciju, koja uključuje i korišćenje interneta za *download* materijale koji predstavljaju autorska dela, naravno uz prethodno plaćanje „članarine" od strane korisnika sajta koji to čini. Svi oblici „*piraterije*" su veliki problem svih država bez diskriminacije, koja bi se mogla učiniti logičnom s obzirom na razlike u njihovoj razvijenosti, zakonodavstvu i rigoroznosti državnih organa koji bi ovu pojavu trebalo da spreče. Piraterija modernog doba je uistinu globalan fenomen, budući da gotovo da nema tačke na planeti na kojoj računarska tehnologija i internet nisu poznati. Pribavljena uz minimalne troškove, autorska dela se mogu prodavati po cenama koje su desetak puta niže od tržišne, a ipak donositi ogromnu zaradu. Zarade od ovakvih poslova, prema nekim procenama, mogu da „ugroze" i zarade od prodaje narkotika, što dovoljno govori o masovnosti ovih pojava.

Međutim, za pojavu neovlašćenog distribuiranja autorskih dela karakteristična je i druga dimenzija razvoja savremenih tehnologija, koja se ogleda u filozofiji da svakom pojedincu treba pružiti podjednake šanse za upoznavanje i rad na računarima s najnovijim programima i da velike kompanije koje imaju monopolski položaj u pojedinim granama proizvodnje npr. računarskih programa, na svojim proizvodima ostvaruju (procentualno) daleko veću zaradu nego što to čine kompanije u drugim granama industrije. Na taj način, bavljenje računarima, ili bavljenje određenim profesijama koje se danas ne mogu zamisliti bez upotrebe računara i određenih računarskih programa, postaje privilegija bogatih. Zbog toga, oni distribuciju takvih proizvoda, koje su prethodno „obradili", odnosno lišili tehničke zaštite postavljene zbog zaštite autorskih prava, ne rade iz lukrativnih pobuda. Takvi programi se mogu naći potpuno besplatno na internetu ili lokalnim mrežama.

Druga karakteristika vredna pomena na ovom mestu tiče se razvoja različitih računarskih mreža koje ne koriste internet sajtove za skidanje nelegalnog sadržaja, već posebne računarske programe pomoću kojih se njihovi računari direktno „umrežuju" i pomoću kojih mogu direktno deliti sve računarske programe i druge legalne i nelegalne sadržaje, a da se pri tome ne može ući u trag njihovoj razmeni, odnosno sadržini podataka koju su dva računara razmenila. Ovaj postupak je zloupotreba podržavane i popularne ideje da se korisnici sličnih interesovanja mogu umrežavati radi razmene korisnih informacija i drugih sadržaja naučne, zabavne i druge sadržine.

Konvencija o visokotehnološkom kriminalu Saveta Evrope ne posvećuje mnogo prostora ovom problemu, pre svega zato što u oblasti zaštite autorskih i srodnih prava postoje odgovarajući međunarodni dokumenti, čiji je domašaj sada proširen i na izvršenje inkriminisanih dela korišćenjem računara i računarskih mreža.

Konačno, treba napomenuti da zakonodavstva najvećeg broja zemalja prepoznaju kao krivično delo proizvodnju, pribavljanje radi prodaje, prodaju i druge načine distribucije, ali ne i kupovinu i upotrebu ilegalnih računarskih programa i drugih autorskih dela od strane fizičkih lica. Količina koja razdvaja posedovanje radi lične upotrebe od posedovanja radi dalje distribucije nije još jasno određena. Većina zemalja koristi kombinovanu metodu vrednosti falsifikata i fizičkog broja kopija koje se nađu u posedu pravnog ili fizičkog lica.

3) Akti rasističke i ksenofobične prirode

Razvoj računarskih sistema drastično je uticao na brzinu i količinu informacija koju svaki pojedinac može da razmenjuje sa ostatkom sveta koji poseduje odgovarajuću tehniku. Danas, različite internet prezentacije, čak i one lokalnog sadržaja, imaju od nekoliko stotina, pa do nekoliko stotina hiljada posetilaca na mesečnom nivou. Osim očiglednih dobrih strana ovakvog razvoja – upoznavanje različitih kultura, dostignuća, bolja informisanost iz različitih izvora i slično, internet nosi i opasnost od širenja ideja koje su označene kao društveno opasne i nepoželjne i koje se ne mogu tako lako diseminirati klasičnim načinima širenja propagande. Reč je, između ostalog, i o širenju rasne, verske, nacionalne i drugih oblika mržnje i netrpeljivosti, pre svega postavljanjem prezentacija na internetu koje ili veličaju fašističke, nacističke i slične ideje, ili o određenim kategorijama ljudi govore sa očiglednim predrasudama, neretko i svesno ulazeći u neistine i uz isticanje ideja o fizičkoj eliminaciji takvih grupa, odnosno pojedinaca. Svaka država je potpisnica međunarodnim dokumenata o ljudskim pravima i zabrani diskriminacije i dužna je da ovakve pokušaje spreči i adekvatno kazni. Ali kako sprečiti pojavu pokušaja širenja ideja mržnje preko interneta? Ovaj problem je poslednjih godina postao veoma aktuelan, pre svega zato što je postavljanje osnovne internet prezentacije usavršavanjem korisničkih programa i omasovljavanjem interneta postalo tehnički jednostavno i finansijski prihvatljivo, čak i za pojedince koji nemaju veće izvore prihoda (ili ih nemaju uopšte, kao što je slučaj na primer s maloletnicima ili nezaposlenim licima, licima koja optužena za neko krivično delo i nalaze se u bekstvu i sl.).

Jedan od odgovora međunarodne zajednice je i potpisivanje dodatnog protokola uz Konvenciju o visokotehnološkom kriminalu Saveta Evrope 2003. godine. Protokol poznaje četiri moguća oblika rasističkog ili ksenofobičnog ponašanja preko računara ili računarskih sistema: rasturanje rasističkog ili ksenofobičnog materijala preko računarskih sistema, rasno motivisanu pretnju, rasno motivisanu

uvredu, kao i delo poricanja, značajnog umanjivanja, odobravanja ili pravdanja genocida ili dela protiv čovečnosti. Državama-potpisnicama ostavljena je sloboda da li će poslednja dva dela uvrstiti u nacionalno zakonodavstvo. Protokol sadrži i odredbu prema kojoj potpisnice neće morati da bilo koje od ovih dela uvrste u zakonodavstvo ako su ona već na prikladan način predviđena njihovim važećim propisima. U svakom slučaju, reč je o pokušaju da se na nadnacionalnom nivou reguliše ovaj problem korišćenjem već postojeće veze između država koje su potpisnice Konvencije o visokotehnološkom kriminalu.

4) Dečja pornografija

Ovde je reč o još jednom delu koje nije „originalno" delo visokotehnološkog kriminala, ali je internet omogućio da se ono razvije do neslućenih dimenzija. Ujedno, ovo je jedno od dela (slično stavljanju sadržaja rasističke prirode na internet prezentacije) za koje nije potrebno značajno znanje o rukovanju računarima, tako da ga može počiniti svako ko je povezan na neku računarsku mrežu. Najkraće rečeno, dela dečje pornografije predstavljaju nelegalni sadržaji na kojima su predstavljeni aktovi dece, ili deca u bilo kakvom seksualnom kontekstu, koji su dostupni drugim licima. Motiv ne mora biti lukrativan – besplatni sadržaji su isto tako nelegalni kao i oni za koje se plaća. U ranim fazama razvoja interneta ovo delo se uglavnom izvršavalo tako što su se stavljali oglasi o prodaji kompakt diskova s dečjom pornografijom. Ovakav pristup je omogućavao policiji da relativno efikasno deluje – policajac koji bi se predstavio kao zainteresovani potencijalni kupac stupio bi u lični kontakt sa osobom koja je prodavala ovakve sadržaje i prilikom pokušaja prodaje bi je uhapsio.[13] Danas, tako nešto se događa isključivo kao izuzetak, a pravilo je da se ovakvi sadržaji prenose putem umrežavanja korisnika. Na taj način se veoma teško može uočiti izvršenje ovog dela – sadržina razmene između dva (ili više) računara je privatna komunikacija koja se ne može presresti bez razloga. Čak i kada postoje razlozi i osnov presretanja, danas se u svakom trenutku putem različitih korisničkih programa vrši umrežavanje računara koji prenose ogroman broj informacija, od kojih je većina potpuno legalna. Manji procenat nelegalnih, a posebno specifične sadržaje kao što je dečja pornografija, gotovo da je nemoguće otkriti.

Samo delo nije unifikovano kada je reč o inkriminacijama u različitim zakonodavstvima. Uglavnom postoje dve razlike u pristupu. Prvo, neke zemlje inkriminišu samo činjenje dostupnim (pod kojim se podrazumeva i prodaja) ovih sadržaja, dok druge smatraju kažnjivim i posedovanje.[14] Druga razlika je još

13 Ovakva akcija policije je izvedena i u Srbiji 2006. godine. Branislav Grković, *Sajber kriminal – zlostavljači iz anonimnosti*, „Vreme", 08. februar 2007. godine. Ceo tekst može se pročitati i na internet adresi http://www.netnovinar.org/netnovinar/dsp_page.cfm?pageid=437&articleid=8831&url sectionid =1375&specialsection=ART_FULL, 03.10.2007

14 Iako se zabrana posedovanja ovakvog materijala ne može dovesti u pitanje, nacionalna zakonodavstva, po pravilu, ne prave razliku kad je u pitanju količina materijala koji je nađen na nečijem

drastičnija: dok većina zemalja iskorišćavanje dece za snimanje ovakvih sadržaja izdvaja kao posebno, izuzetno teško krivično delo, zakonodavstva manjeg broja zemalja korišćenje (mučenje) dece u te svrhe povezuju s kasnijom distribucijom (i/ili posedovanjem) dečje pornografije – i oba postupka posmatraju kao lakša krivična dela. U drugom slučaju, pozitivna može biti samo činjenica da se korišćenje dece radi snimanja slika ili video zapisa pornografskog sadržaja posmatra u sticaju s drugim krivičnim delima (silovanje, seksualni odnos s licima mlađim od određenog uzrasta, protivpravno zadržavanje lica, otmica), pa je moguće izreći kaznu (kumulativnu ili jedinstvenu, u zavisnosti od pravnog sistema) koja odgovara težini ovakvog postupanja. Ipak, čini se da visokotehnološkom kriminalu pripada samo distribucija i posedovanje ovih sadržaja, dok se njihova proizvodnja mora inkriminisati kao posebno krivično delo za koje su predviđene daleko strože kazne.

Neophodno je i napomenuti da ova vrsta krivičnih dela nije na jedinstven način regulisana u različitim zakonodavstvima kada je reč o starosti osoba koje se nalaze u materijalima pornografske sadržine. Tu do izražaja dolaze i civilizacijske i kulturne razlike, pa granica varira od 14 godina do 21 godine starosti. Iz istih razloga, i pojedine države još nisu ni prihvatile inkriminaciju ovih postupaka.

Uvidevši ozbiljnost i rasprostranjenost ovog problema, Evropska konvencija o visokotehnološkom kriminalu pokušava da autoritativno „navede" države da harmonizuju svoja zakonodavstva i na taj način doprinesu njegovom suzbijanju. Ne samo što su sve države u obavezi da inkriminišu različite oblike proizvodnje, posedovanja i distribucije dečje pornografije, već Konvencija sadrži i neke odredbe koje su mnogo obuhvatnije od svih uporednih rešenja u nacionalnim zakonodavstvima. Tako je najpre starosna granica do koje se osobe smatraju decom postavljena na 18 godina, uz mogućnost da države individualno odluče da je smanje na 16 godina starosti. Potom su inkriminisani sadržaji u kojima se pojavljuju osobe za koje se može osnovano pretpostaviti da su mlađe od 18 godina, ili se predstavljaju kao takve, kao i drugi grafički sadržaji (crteži, crtani filmovi i slično) u kojima se predstavljaju osobe mlađe od propisane granice u pornografskom kontekstu. Ipak, Konvencija ostavlja mogućnost stavljanja rezervi na takva rešenja, čime se ne doprinosi unifikaciji zakonodavstava u ovoj oblasti.

Ono što ni Konvencija ni nacionalna zakonodavstva ne rešavaju efikasno jeste pitanje kako inkriminisati upotrebu savremenih tehnologija od strane samih lica koja se ovim odredbama štite? Najčešće se može primeniti neka od odredbi koje se inače nalaze u okviru inkriminacija ostalih seksualnih delikata,

---

računaru ili bilo kom drugom nosaču informacija. Nije neverovatna situacija da neko, na primer, prima svakodnevne (ili periodične) neželjene elektronske poruke (*e-mail*) koje sadrže reklamu neke internet prezentacije sa ovakvim sadržajem i u okviru takve reklame nekoliko primeraka fotografija i video zapisa. Ukoliko se takva pošta automatski preko korisničkog programa za pregled *e-maila* sortira u poseban folder za neželjenu poštu, korisnik računara čak ne mora biti ni svestan postojanja ovakvog sadržaja. Da li je on kriminalac? Prema nekim zakonodavstvima, odgovor bi morao da bude pozitivan, što je nelogično i kontraproduktivno rešenje.

kao i krivične (ne)odgovornosti maloletnih osoba. Čini se da se mora najpre precizno utvrditi donja granica kažnjivosti takvih postupaka, koja mora biti u skladu sa ostalim krivičnim delima iz ove oblasti. Potom se mora jasno odrediti društveni stav prema onim delima koja bi i prema tako utvrđenim granicama spadala u kažnjiva – čini se da u ovom slučaju klasične krivičnopravne sankcije ne dolaze u obzir i da se pre svega mora mobilisati porodica i šire okruženje takvih lica da bi se ovakvi problemi rešili. Obrazovno-vaspitne ustanove do sada, po pravilu, nisu adekvatno reagovale, a često nisu reagovale uopšte, iako su imale saznanja o postojanju slučajeva dečje pornografije koja se ne samo distribuirala u školi, nego je tamo i proizvedena.[15]

5) Računarske prevare

Najmaštovitija i najširа grupa krivičnih dela koja se mogu izvršiti korišćenjem računarskih mreža su različiti oblici prevara. Evropska konvencija o visokotehnološkom kriminalu poznaje samo dva oblika ovakvih dela: falsifikovanje i prevaru, oba u slučaju kada su povezani sa upotrebom računara. Na taj način, domašaj Konvencije je učinjen veoma ograničenim i nacionalna zakonodavstva moraju otići korak dalje u regulisanju ove vrste visokotehnološkog kriminala. Treba najpre razlikovati one vrste prevara kod kojih je računar samo sredstvo komunikacije kriminalca i žrtve od onih koje zahtevaju visokotehnološko znanje i tehnologiju da bi mogle biti realizovane.

U prvu grupu spada jedna od najpopularnijih prevara koje su ikada izvedene putem i-mejla – „nigerijsko pismo". Prevara je veoma jednostavna. Koristeći lakovernost ljudi, šalje im se „poverljivo" pismo od izvesnog gospodina iz Afrike (prva pisma su koristila Nigeriju kao zemlju porekla poruke, otuda i naziv ove prevare) koji se našao na udaru „revolucionarne pravde" i koji mora smesta svoje ogromno bogatstvo da prebaci na sigurne račune u Evropi. Najčešće su u pitanju sume od nekoliko stotina miliona dolara, od kojih je dotični gospodin spreman da izdvoji određeni procenat (5–20%, ponekad i više), ali postoji problem – na određeni račun treba smesta uplatiti izvesnu sumu novca kao garantiju veće uplate (ili kao naknadu troškova banci i slično). Gospodin u nevolji nikako nije u mogućnosti da tu transakciju realizuje, ali je preko „poverljivih izvora" saznao da ste baš vi čovek od izuzetne diskrecije i poverenja i moli vas da mu pomognete uplatom na taj-i-taj račun... Sume koje su na ovaj način uzimane lakovernim ljudima su se kretale od 100 do 1.500 $, a prevaranti nisu bili izbirljivi – ovakve poruke su upućivali na hiljade adresa, ostvarujući tako ponekad i neslućenu zaradu. Ljudi koji su prevareni najčešće nisu želeli da se za njihovu lakovernost sazna

15 Gotovo da se ne može naći država u Evropi (sasvim sigurno i šire) u kojoj ne postoje internet prezentacije na kojima su dostupni ovakvi sadržaji, iako su po nekim krivičnim zakonodavstvima stavljeni van zakona. U Srbiji je poznat slučaj iz Kragujevca, kada su „akteri" video zapisa snimljenih mobilnim telefonom čak došli na naslovne strane pojedinih dnevnih novina.

i odricali su se tih suma novca ne prijavljući policiji šta se dogodilo. Čak i kada bi prijavili, često je od same uplate do saznanja da od „procenta" od milion dolara nema ni govora proteklo nekoliko meseci, što je više nego dovoljno da prevaranti zametnu svoje tragove.

E-mail prevare su toliko česte da bi se samo o njima mogla napisati posebna studija. Na ovaj način se reklamiraju proizvodi koje ljudi obično ne žele da kupuju u javnosti – lekovi, nedozvoljene supstance, seksualna pomagala, poslovna pratnja – lista je beskonačna. Takođe, moli se za pomoć bolesnoj deci, gladnima u Africi, žrtvama cunamija u Aziji... Prema istraživanjima, sprovedenim u 2006. godini, oko 90% sve elektronske pošte koja stigne prosečnom korisniku interneta je „neželjena pošta" (eng. *spam*) u kojoj se kriju različite poruke koje vas mogu odvesti u svet internet prevara.[16]

Međutim, suština prevare korišćenjem savremenih tehnologija nije samo u novim mogućnostima masovne komunikacije s nepoznatim ljudima i korišćenjem njihove dobrote, lakovernosti i ostalih ljudskih osobina koje su karakteristične i za „klasične" obmane. Još od sedamdesetih godina XX veka, kada je jedan student otkrio da se (tadašnji) računari mogu koristiti za obavljanje telefonskih poziva bez naplate,[17] razvio se čitav niz zloupotreba. Najčešće su zloupotrebe vezane za plaćanje ukradenim kreditnim karticama, kao i druge finansijske malverzacije koje su, po pravilu, posledica prethodnog počinjenog drugog krivičnog dela – neovlašćenog pristupa informacijama na tuđem računaru, na primer. Ovakvom načinu prevare blisko je slično „preuzimanje identiteta", „predstavljanje" kriminalaca na računarskoj mreži kao neke druge osobe.[18]

Osim ovih prevara, postoje i prevare koje su vezane za *spoofing*, radnju za koju još nema ekvivalentnog prevoda na srpskom jeziku, a koja se sastoji od slanja elektronskih poruka s tuđe adrese (što se svodi na „preuzimanje identiteta"), ili sa *e-maila* koji podseća na originalnu adresu. Svrha ovakvog postupka je da adresant poruku shvati ozbiljno, da ona ne završi u njegovoj neželjenoj pošti. Na taj način se on dovodi u zabludu o tome ko mu piše, i kriminalac lakše s njim gradi odnos poverenja koji dovodi do konačnog izvođenja prevare.[19] U ovu vrstu

16 Brian Krebs, *Year of Computing Dangerously*, Washington Post, 22.12.2006, http://www.washingtonpost.com/wp-dyn/content/article/2006/12/22/AR2006122200367.html, 03.10.2007

17 Ova pojava je nazvana „friking" (eng. *phreaking*, što je skraćeni oblik dve reči – *phone* i *freaking*). Iako se smatra „klasičnom" računarskom prevarom za čije su suzbijanje telefonske kompanije uložile značajna sredstva, friking je i danas veoma rasprostranjen u svim državama sveta.

18 Klasičan primer vezan je za tzv. *e-banking*, obavljanje bankarskih transakcija putem računarskih mreža. Osoba koja poseduje određene podatke (korisničko ime, lozinku) nekog korisnika *e-banking*a, može pristupiti njegovim bankovnim računima i prebacivati novac na druge račune.

19 Na primer, poznate su elektronske poruke koje kruže internetom u ime Citizen banke. Ovde je očigledna analogija sa City bankom iz SAD, jednom od najvećih banaka na svetu. U ovakvim porukama se budućim „korisnicima" za otvaranje računa i druge transakcije koje bi obavili nude različite pogodnosti, uz neizbežno posredovanje neke treće banke (u kojoj počinioci dela imaju otvoren račun). Citizen banka ne postoji, a bankovni račun preko kojeg se navodne transakcije obavljaju (a koji se nalazi u nekoj trećoj banci) odmah po izvršenoj prevari počinioci prazne i gase.

krivičnih dela spada i pravljene lažnih, „jednokratnih" internet prezentacija koje navodno predstavljaju poznate kompanije iz najrazličitijih oblasti privređivanja. Ovakve prezentacije se po izvršenoj prevari gase, a počinioci po pravilu koriste i internet adresu i vizuelni izgled na osnovu koga se ne može posumnjati da se radi o prevari.[20]

6) Ostala dela koja uključuju korišćenje računara i računarskih mreža

Ostala krivična dela koja se mogu izvršiti korišćenjem računara ili računarskih mreža uglavnom se svode na nekoliko potpuno različitih grupa delovanja:

- *Povreda prava na zaštitu privatnih podataka o ličnosti* – nije nepoznato da se provajderi internet i drugih usluga mogu protivpravno služiti informacijama kao što su *e-mail*, podaci o sajtovima koje posećujete i sl. Ovi podaci se prodaju ili ustupaju različitim kompanijama, koje ih koriste da bi na poštansku adresu ili *e-mail* korisnika računara slali reklamni materijal, ili za formiranje profila ličnosti koji znatno pomaže pristupu u slučaju različitih prevara.[21] Kada osoba sakuplja podatke do kojih može doći preko računarskih mreža da bi stupila u bilo kakav (pismeni, usmeni, direktni) kontakt s drugom osobom, može se govoriti o tzv. *„sajber-uznemiravanju"*.

---

20 Najpoznatija prevara ove vrste je izrada prezentacija velikih firmi koje se bave proizvodnjom korisničkih programa (npr. Microsoft). Prevara se najčešće izvodi tako što se dolaskom korisnika računara na odgovarajuću internet prezentaciju u njegov računar ubacuje određeni program koji ne detektuju konvencionalni programi zaštite, a koji se manifestuje u izbacivanju reklamnih poruka ili sličnih postupaka koji opterećuju kako računar, tako i njegovog korisnika. Naravno, ubrzo na *e-mail* korisnika dolazi „spasonosna" poruka od Microsofta da se *downloadom* novog korisničkog programa efikasno eliminišu sve takve maliciozne tvorevine na računaru. Korisnik odlazi na preporučenu internet prezentaciju, koja neobično podseća na originalnu, kupuje preporučeni korisnički program i – prevara je izvršena. Slanjem ogromnog broja ovakvih poruka na prethodno „zaražene" računare, prevaranti mogu u roku od samo nekoliko dana zaraditi ogromne svote novca. Tada lažna internet prezentacija „nestaje", a kupljeni programi koji navodno rešavaju korisnike računara nevolje koju su im sami autori tih programa nametnuli, u zavisnosti od malicioznosti počinioca ovog dela, stanje čine još gorim, ili ga vraćaju u prvobitno stanje. Za prevarante kojima je ovakav vid obmane i suviše komplikovan, postoje i znatno lakši načini – postavljanjem „originalne" prezentacije nekog popularnog fudbalskog kluba i *on-line* „prodajom" sezonskih karata po znatno nižoj ceni od uobičajene takođe se mogu zaraditi znatne sume novca u roku od nekoliko dana.

21 Ovi podaci se mogu koristiti na različite načine koji uopšte nisu povezani sa internetom ili računarima, već koriste druge savremene tehnologije. Na primer, veliki lanci prodavnica robe široke potrošnje imaju svoje posebne kartice, kojima korisnici ostvaruju posebne popuste prilikom kupovine. Međutim, svaki put kada neka osoba iskoristi tu karticu (ili čak bilo koju kreditnu karticu) pri kupovini, podaci o tome koje je proizvode kupila prodavnice šalju proizvođačima, koji ih koriste da bi reklamirali određene grupe svojih proizvoda ciljnim grupama. Na primer, ako kupite više puta hranu za pse, postoji velika verovatnoća da će vam na kućnu adresu uskoro stići katalog s hranom i najrazličitijim predmetima vezanim za kućne ljubimce. Na ovaj način se krši pravo na zaštitu podataka, ali i pravo na privatnost, odavanjem kućne adrese i kršenjem odnosa poverljivosti između prodavca i kupca. Ipak, ova dela ne spadaju uvek u nedozvoljeno ponašanje – u mnogim zakonodavstvima nisu inkriminisana i ne povlače (krivičnopravne) posledice.

- *Prikupljanje podataka koji su označeni kao tajni* – moderna špijunaža se obavlja gotovo isključivo savremenim tehnologijama. Sateliti koji prate kretanje i lociranje određenih ljudi ili objekata, baze podataka u koje se može neautorizovano ući, predstavljaju glavna „oružja" savremenih špijuna, koji na ovaj način dolaze do vojnih i državnih tajni, kao i do važnih industrijskih podataka i patenata.
- *Prodaja nelegalnih supstanci i drugih predmeta preko računarskih mreža* – o ovim delima je već bilo reči. Ono što ih razlikuje od internet prevara jeste da se u ovom slučaju kupoprodaja zaista odvija, ali je njen predmet neka supstanca ili druga stvar koja se ne može naći u pravnom prometu, ili se može naći samo uz posebnu dozvolu države (koja, naravno, u ovom slučaju ne postoji). Lekovi, eksploziv, planovi i udžbenici za pravljenje hemijskih otrova, ali i kradena umetnička dela, automobili, druge dragocenosti – mogu biti predmet jednog ovakvog nelegalnog posla. U većini slučajeva je notorna činjenica da je supstanca ili predmet koji je predmet kupoprodaje ilegalan ili ukraden, ali postoje i slučajevi kada kupac to ne može znati – tada je ovakva prodaja bliža opisanom delu prevare.

3. ODNOS VISOKOTEHNOLOŠKOG KRIMINALA SA ORGANIZOVANIM KRIMINALOM I TERORIZMOM

Odnos visokotehnološkog i organizovanog kriminala može se posmatrati iz dva aspekta: kao organizovanje sajber-kriminalaca i kao korišćenje savremenih tehnologija u aktivnostima „klasičnog" organizovanog kriminala. U drugom slučaju, radi se o elektronskim transakcijama, tokovima novca koji se teško prate ako se pripadnici organizovanog kriminala služe novim pogodnostima za transfer ili „pranje" novca stečenog nelegalnim aktivnostima.[22]

Prva aktivnost je daleko zanimljivija kada se izučava visokotehnološki kriminal. Da li je moguće kriminalno udruživanje pojedinaca ili grupa u virtuelnom prostoru? Da, ali ne onako kako bi to pojedinci verovatno sebi predstavili. Najjednostavnije rečeno, kada neki pojedinac ima „kvalitetnu" ideju o tome kako izvesti određenu prevaru, a nema dovoljno finansijskih sredstava ili opreme, ili jednostavno želi da smanji rizik od hapšenja za 50%, udružiće se s drugim pojedincem.[23] Ono što je u ovakvoj „organizaciji" poseban kuriozitet – njeni članovi se nikada ne moraju videti, niti znati identitet, izgled, ili bilo koji privatni podatak drugih osoba s kojima su na ovaj način povezane. Drugi način ovakve organizacije predstavlja

22 Do sada najveća i najpoznatija afera u vezi s pranjem novca korišćenjem savremenih tehnologija dogodila se 2000. godine, kada je ogranak sicilijanske mafije pokušao da „opere" oko 400 000 000 dolara preko Banke Sicilije, uz posredovanje niza banaka u Portugalu, Švajcarskoj i Banke Vatikana. Prevara je otkrivena samo zato što je jedan od učesnika u pranju novca odao policiji ceo plan. Više o ovom i sličnim primerima: Phil Wiliams, *Organized Crime and Cybercrime: Synergies, Trends, and Responses*, http://www.crime-research.org/library/Cybercrimehtm, 03.10.2007.

23 Zanimljiv primer o ovakvom udruživanju: Robert Vamosi, *Cybercrime does pay; here's how*, http://reviews.cnet.com/4520-3513_7-6427016-1.html, 03.10.2007

organizovanje sajber-kriminalca, najčešće pod okriljem neke grupe organizovanog kriminala, koja želi da proširi svoje delovanje i na internet prevare. Takve grupe se prepoznaju najpre po masovnosti prevara koje obavljaju, ali njihovi metodi se ne razlikuju mnogo od onih koje koriste pojedinci. Takođe, ovakve grupe obavljaju isključivo lukrativne prevare, dok se ne bave onima koje su pojedini hakeri radili „za slavu", odnosno da bi preneli neku političku ili sličnu poruku.[24]

Kada je reč o odnosu sajber-kriminala i terorizma, mora se reći da savremene tehnologije (računarske i druge) nude obilje mogućnosti za teroriste da svojim nelegalnim aktivnostima sabotiraju svakodnevni način života i bezbednost građana. Na primer, obaranjem računarske mreže nekog aerodroma može se izazvati zastoj u avionskom saobraćaju, kao i značajni finansijski gubici, neautorizovano uticati na bilo koji računarski sistem državnih institucija, berze i sl. Konkretnije, mada više u domenu telekomunikacione nego računarske zloupotrebe savremenih tehnologija, dokazano je da su u različitim terorističkim napadima širom sveta mobilni telefoni korišćeni kao okidač – inicijator eksplozija. Kako se tehnologije razvijaju, mogućnosti postaju šire i drastičnije.[25]

Drugi aspekt povezanosti visokotehnološkog kriminala i terorizma je u komunikaciji i transferu podataka, novca, logistike putem interneta i drugih računarskih mreža. Jednostavno, internet je komunikaciju između različitih delova sveta učinio ne samo jednostavnijom i jeftinijom, već i mnogo težom za prisluškivanje i praćenje. Milijarde elektronskih poruka koje kruže računarskim mrežama svakodnevno ne mogu se u potpunosti ispratiti, dok je samo presretanje ovakvih vrsta komunikacije zakonski zaštićeno i ne može se vršiti bez osnova i odgovarajuće procedure. Zato nije nerealno reći da postoji veza između savremenih tehnologija i terorizma, kao i da dobro obučeni teroristi mogu ponekad na sebe preuzeti ulogu sajber-kriminalaca radi ostvarivanja nekog zadatka. Previše bi, međutim, bilo izvesti ovakav zaključak van okvira realnosti. Ljudi koji se bave visokotehnološkim kriminalom rade to pre svega iz finansijskih pobuda; daleko je manji broj onih koji to čine iz nekih političkih, religijskih i drugih ubeđenja.

4. PROBLEMI PROCESNOPRAVNE PRIRODE

Visokotehnološki kriminal je relativno nova pojava u svetu i mnoge države i međunarodne organizacije nisu još adekvatno reagovale na njegovo značajno širenje poslednjih godina. Osim Evropske konvencije o visokotehnološkom kriminalu, nema ozbiljnijeg međunarodnog dokumenta koji bi regulisao neka pitanja na globalnom nivou. Istovremeno, ne postoji ni jednoobrazna, nedvosmislena praksa nacionalnih sudova oko važnih pitanja koja se tiču nadnacionalnog elementa,

24 Izvor: http://www.wired.com/techbiz/media/news/2006/09/71793, 03.10.2007

25 Poznato je da sve savremene fabrike vode koriste računare za njenu preradu – i na ovaj proces se može uticati (pre svega u smislu njegove destrukcije, odnosno zastoja u proizvodnji) neovlašćenim pristupom takvim računarskim mrežama.

ali ni kada je reč o nekim praktičnim problemima koji su, čini se, neminovni prilikom procesuiranja ovih dela pred sudom. Zbog navedenih, ali i drugih činjenica koje čine visokotehnološki kriminal specifičnim, postoji niz problema. Ukazaćemo na neke:

- Kako goniti delo koje je „izvršeno" u nekoliko država istovremeno? Veliki broj krivičnih dela iz ove oblasti vezan je svojom prirodom za više od jedne države, a kombinacije koje pri tome mogu nastati su gotovo beskonačne – na primer, državljanin Španije izvrši prevaru preko internet prezentacije koja se nalazi na serveru u Norveškoj, dok su oštećeni iz Kanade i Belgije. Verovatno najpoznatiji primer ovog tipa dogodio se nedavno u Austriji, prilikom akcije protiv vlasnika internet prezentacije s dečjom pornografijom. Vlasnik je austrijski državljanin, ali je server na kome se prezentacija nalazila zakupljen u Rusiji (provajder je dao dojavu austrijskoj policiji kada je uvideo da se prezentacija koristi za nelegalne radnje i na taj način inicirao istragu i potonja hapšenja). Korisnici prezentacije, koji su takođe počinili krivično delo jer su plaćali za dobijanje korisničke lozinke za pregled sadržaja prezentacije, uglavnom su iz Velike Britanije i Danske. Ovde je situacija (gotovo) jasna, budući da su nadležni organi različitih država sarađivali u celom poduhvatu – vlasniku prezentacije će se suditi u Austriji, a ostalim okrivljenim u zemljama čiji su državljani. Situacija ne mora međutim uvek biti takva, a čak i ovaj slučaj povlači još jednom veliko pitanje, odnosno problem: kako goniti počinioce dela koje u državama čiji su državljani ili na čijoj su teritoriji izvršena nije kažnjivo? Odgovor je, nažalost – nikako. Ukoliko postoji mogućnost, država koja želi da zasnuje nadležnost može tražiti ekstradiciju, ali nijedan međunarodni dokument ne poznaje mogućnost ekstradicije u pomenutom slučaju. Ove „sigurne države" većinom imaju manjkavo zakonodavstvo, i to ne zbog svoje politike nekažnjavanja visokotehnološkog kriminala, već zbog neprepoznavanja društvene opasnosti koju on nosi. Jedan od rasprostranjenih razloga je i relativna nerazvijenost zemlje u pogledu savremenih tehnologija, kao i nedostatak stručnjaka koji bi se mogli baviti ovom problematikom.
- Relativnost načela *ignorantia iuris non excusat* – bez ikakve namere da se opovrgne ovo fundamentalno pravilo, mora se ukazati da „počinioci" pojedinih dela ne moraju biti svesni toga šta čine niti imati nameru da bilo kome naude ili steknu određenu protivpravnu imovinsku (ili drugu) korist. Dešavalo se da prijatelji na internetu šalju jedan drugome različite forme računarskih virusa, da bi testirali svoju zaštitu. Dešavalo se da putem elektronske pošte ljudi dođu u posed nelegalnog materijala koji dalje distribuiraju, npr. njihove omiljene pesme (koja, naravno, nije legalno kupljena). Ukoliko se javljaju kao usamljena aktivnost pojedinca a ne njegova svakodnevna praksa, ovakvi incidenti ne predstavljaju društvenu opasnost. O tome se pre svega mora voditi računa prilikom donošenja odluke da li treba povesti sudski postupak, što nije uvek slučaj – pojedine države praktikuju veoma strogu kaznenu politiku kao deo preventive daljeg širenja visokotehnološkog kriminala u najširim krugovima stanovništva.

- Međutim, da bi se u samom postupku pravilno odvagale okolnosti slučaja, sudija mora imati zavidno predznanje o stvarima o kojima je reč. Isto se odnosi i na tužioca, kao i na ostale državne institucije koje učestvuju u postupku. Ipak, gotovo nijedna država ne poznaje specijalizaciju i posebnu obuku sudija i ostalih učesnika u suzbijanju visokotehnološkog kriminala, iako je u mnogim postupcima praksa pokazala da veštaci ne mogu interpretirati činjenice na način koji bi sudija bez ikakvog predznanja mogao da shvati u dovoljnoj meri da na osnovu njih odluči o nečijoj krivičnoj odgovornosti.
- Kako biti siguran ko je počinilac dela? Iako ovo pitanje može delovati trivijalno, neko može i „preuzeti" računar bez znanja vlasnika, čak i u trenutku kada vlasnik radi na tom računaru. Kako rešiti ovaj problem ako okrivljeni tvrdi da nije učinio delo za koje se tereti, posebno kada sve okolnosti, a naročito njegovo znanje rada na računaru, ne indikuju da je on učinilac? Ovde dolazimo do novog problema. Temeljnost istražnih radnji iziskuje specifično obrazovanje tužioca i policijskih organa koji sprovode istragu. Većina računarskih prevara je dovedena do takvog oblika savršene manipulacije tuđim računarima da se mora veoma pažljivo postupati sa eventualnim osumnjičenima dok se ne dođe do nedvosmislenog saznanja da su oni na bilo koji način mogli biti umešani u izvršenje krivičnog dela.
- Kako postupati s maloletnim učiniocima? Naravno, sva zakonodavstva imaju posebnu regulativu u slučaju da su počinioci delimično ili potpuno neodgovorni sa stanovišta krivičnog prava, ali su pitanja koja se postavljaju kako moralne tako i praktične prirode – kako objasniti mladim (ponekada i veoma mladim) počiniocima da je npr. slanje kompjuterskog virusa u određenu računarsku mrežu kažnjivo i da može izazvati ogromnu materijalnu štetu? Kako ih kazniti (ili – da li ih kazniti?), ali kako i sprečiti ponavljanje izvršenja ovakvih krivičnih dela? Instituti klasičnog krivičnog prava koji su na raspolaganju državnim organima i institucijama koje brinu o maloletnim osobama najčešće nisu od pomoći u ovakvim slučajevima.
- Prethodno pitanje otvara novi problem, u odnosu na sve počinioce (i potencijalne počinioce): kako raditi na prevenciji izvršenja krivičnih dela iz ove oblasti? Treba naglasiti i drugu stranu ovog problema: kako onemogućiti počinioca da ponovi svoje delo? Kazne koje su se koristile na početku razvoja zakonodavstava pojedinih država o visokotehnološkom kriminalu (kao što je kućni pritvor) jednostavno ne mogu biti efikasne. Zabrana „kontakta" osobe s računarom je takođe besmislena, posebno kada se u vidu ima i hiperrazvoj ovih tehnologija i mogućnost da se mnoga od ovih dela izvrše i uz pomoć neke druge savremene naprave.
- Kako dokazivati delo visokotehnološkog kriminala? Ponekad su podaci koje dostavi internet (ili drugi) provajder dovoljni da se neko lice poveže sa određenim krivičnim delom. Kada oni nisu dovoljni, koliko je validno prihvatiti sadržaj hard diska, fleš memorije ili drugih medijuma pred sudom, posebno u slučaju kada sudija ne zna šta je hard disk i ne može valjano da proceni da li se može prihvatiti kao dokaz, kao i težinu takvog dokaza?

- Takođe, u vezi s dokazivanjem dela, pitanje koje je poslednjih godina veoma aktuelno jeste kako „slušati" komunikacije, a ne ugroziti pravo na privatnost pojedinca? Za razliku od istrage povodom drugih krivičnih dela gde npr. prisluškivanje telefona dolazi kao mera kojoj prethode neke druge istražne radnje koje bi identifikovale da je neko lice umešano u protivpravno delovanje, kod visokotehnološkog kriminala se ponekad ne može utvrditi jasna granica kada postoji sumnja, odnosno kada je traženje pojedinih privatnih podataka o ličnosti dozvoljeno i uopšte relevantno za istragu. Ovaj problem ne dolazi od tendencije policijskih i drugih organa da svoja ovlašćenja tumače široko. Naprotiv, sama priroda visokotehnološkog kriminala je takva da je on „skriven" i da je potrebno značajno znanje i iskustvo da bi se uopšte percipirao.

5. JOŠ NEKOLIKO NAPOMENA O KONVENCIJI O VISOKOTEHNOLOŠKOM KRIMINALU SAVETA EVROPE

O Konvenciji o visokotehnološkom kriminalu je već bilo reči u delu teksta o materijalnom pravu. Inkriminisanje pojedinih akata visokotehnološkog kriminala je ipak predmet samo prvog dela Konvencije, koja uvodi još niz značajnih odredbi koje se tiču procesnog prava i međunarodne saradnje.

Drugi deo pod nazivom „Procesno pravo" bavi se procesnim ovlašćenjima državnih organa prilikom istraživanja krivičnih dela vezanih za nove tehnologije. Osim opštih odredbi koje nalažu državama da u svoje krivično pravo uvedu pomenuta krivična dela, kao i druga dela koja se ne nalaze u tekstu Konvencije a koja se mogu podvesti pod ovu grupu, velika pažnja se posvećuje načinu prikupljanja podataka koji se nalaze na računarima ili prenosnim uređajima, kao i zaštiti osnovnih prava pojedinca garantovanih Evropskom konvencijom o ljudskim pravima i Paktovima o ljudskim pravima UN. Prema Konvenciji, nadležni državni organi imaju ovlašćenja da pregledaju i zaplene svaki računar ili nosač podataka na kome se nalaze, ili sumnjaju da se mogu nalaziti inkriminišući materijali, kao i da od provajdera elektronskih komunikacija prikupljaju podatke koji se odnose pre svega na upotrebu interneta i kreditnih kartica, preko kojih se može doći do imena ili IP adrese[26] potencijalnog počinioca krivičnog dela. Jedna od verovatno najdalekosežnijih odredbi tiče se „presretanja podataka", odnosno neke vrste prisluškivanja elektronskih komunikacija, pre svega onih koje su vezane za internet. Ova oblast intervencije državnih organa je i najosetljivija, jer se praktično povređuje

26 IP adresa je, jednostavno rečeno, vrsta „potpisa" kompjutera koji se konektuje na internet, a koji je jedinstven za svaki računar. Pomoću nje se može doći do lokacije računara s kojeg je počinjeno neko krivično delo. Prema podacima organizacije IPligence (http://www.ipligence.com), trenutno postoji više od milijardu korisnika interneta, dok je broj računara koji imaju pristup internetu višestruko veći. Za više informacija o IP adresi, načinu njenog dodeljivanja i pronalaženja kućne adrese na osnovu IP adrese, videti: tekst *TCP/IP,* na internet stranici http://www.webopedia.com/TERM/T/TCP_IP.html i tekst *IP address,* na internet stranici: http://www.webopedia.com/TERM/I/IP_address.html, 03.10.2007

pravo na privatnost i pravo na prepisku, a Konvencija ne sadrži odgovarajuća ograničenja i garantije da takva prava neće biti zloupotrebljena (osim generalnog ograničenja da se pri izvršenju svih mera moraju poštovati međunarodni standardi ljudskih prava postignuti pomenutim međunarodnim dokumentima).

Treći deo Konvencije bavi se međunarodnom saradnjom država na suzbijanju visokotehnološkog kriminala, i to pre svega na način koji bi trebalo da prevaziđe praktične prepreke pri sprovođenju nacionalnog zakonodavstva za krivična dela koja, po pravilu, prelaze državne granice, a često i podrazumevaju učešće pojedinaca iz nekoliko zemalja širom sveta. Otuda su glavne odredbe ovog dela posvećene saradnji država na razmeni podataka koji se tiču eventualnog izvršenja nekog od krivičnih dela vezanih za upotrebu elektronskih komunikacija, kao i mogućnosti ekstradicije počinilaca takvih dela iz jedne države-potpisnice u drugu. Zanimljiva je i odredba koja se tiče osnivanja „24/7 službe" u svakoj od država, koja bi služila kao podrška policijskim i drugim organima, kao kontakt za sva obaveštenja i početna tačka za sve zahteve koji se tiču procesuiranja i istraživanja krivičnih dela visokotehnološkog kriminala. Time je samo delimično ublažen jedan od glavnih nedostataka Konvencije – državama-potpisnicama nije data obaveza da uvedu posebne organe koji bi se bavili isključivo ovom vrstom krivičnih dela. S obzirom na nužnost specijalizacije policijskih, istražnih, tužilačkih, sudskih i drugih organa pri istraživanju i procesuiranju, čini se da će države morati i bez konkretnih odredbi Konvencije da učine mnogo više od osnivanja „24/7 službe" da bi se efikasno suprotstavile sajber-kriminalcima.

Konvencija je specifična i po jednom nimalo pozitivnom aspektu – razvijene države je nerado ratifikuju.[27] Od zemalja koje možemo nazvati visokorazvijenim kada je reč o savremenim tehnologijama, ratifikovale su je samo SAD 2006. godine (Konvencija je otvorena za potpis i državama koje nisu članice Saveta Evrope), Francuska, Danska i Norveška. Otkuda ovaj otpor? Pre svega zbog pomenutih procesnih ovlašćenja državnih organa, koje Konvencija predviđa i gotovo ne ograničava. EFF[28] je zato naziva „najgorim internet pravom na svetu", koje predviđa da čak i akti koji nisu predviđeni kao krivična dela u SAD mogu biti gonjeni u ovoj zemlji po zahtevu neke druge države u kojoj se smatraju kažnjivim.[29] Ovaj problem postaje još dublji kada se radi o interpretaciji šta se, na primer, može smatrati nedozvoljenim sadržajem na internetu koji ne pokriva sloboda izražavanja – standardi u demokratskim i nedemokratskim zemljama se u tom slučaju

27 Lista ratifikacija može se naći na internet adresi (stanje na dan 03.10.2006): http://conventions.coe.int/Treaty/Commun/ChercheSig.asp?NT=185&CM=1&DF=9/2/2006&CL=ENG

28 EFF (Electronic Frontier Foundation) je jedna od najpoznatijih organizacija koja se bavi zaštitom privatnih podataka u odnosu na nove tehnologije. Više informacija o EFF-u na internet adresi: http://www.eff.org, 27.09.2007

29 Reč je o aktima za koje Konvencija predviđa mogućnost uvođenja u nacionalno zakonodavstvo. Teorijski je moguće da država ne izjavi rezervu na prihvatanje saradnje kada je reč o svim delima predviđenim Konvencijom, a istovremeno neka od njih ne uvede u svoje zakonodavstvo, čime stvara ovakvu, donekle apsurdnu, situaciju.

znatno razlikuju.[30] Činjenica je da se ovakva kategorizacija Konvencije ne može u potpunosti opravdati, ali veoma dobro ilustruje strah od „sudara" potpuno različitih kultura, civilizacija i vrednosti na internetu. Otuda možda i nedostatak relevantnog međunarodnog dokumenta koji bi bio prihvaćen kako na globalnom nivou, tako i od strane najrazvijenijih država sveta.

6. KRATKA ANALIZA ISKUSTAVA POJEDINIH ZEMALJA

Uporednopravna analiza nikako ne može obuhvatiti sve zemlje koje su u poslednjih nekoliko godina aktualizovale ovaj problem. Za razliku od stanja koje je postojalo doskora, danas u svetu gotovo da nema „sigurnih država" za savremene kriminalce. Ipak, razlike u stepenu implementacije su velike – dok neke države imaju posebno zakonodavstvo o visokotehnološkom kriminalu, koje podrazumeva i postojanje posebnih policijskih i drugih jedinica specijalizovanih za njegovo otkrivanje, neke zemlje su se zadovoljile opštim pristupom i uvođenjem pojedinih krivičnih dela koja se tiču nedozvoljene upotrebe savremenih tehnologija. Na ovom mestu ukazaćemo samo na neka od rešenja zemalja iz neposrednog okruženja, kao i zemalja koje imaju izuzetno razvijene sisteme za suzbijanje sajber-zločina.[31]

Hrvatska je dela koja se odnose na visokotehnološki kriminal prvi put unela u zakonodavstvo donošenjem Kaznenog zakona 1997. godine, ali se tek njegovim izmenama iz 2004. godine problemu inkriminacije ovih dela pristupilo detaljno i sistematski, i to pre svega se rukovodeći odredbama Konvencije o visokotehnološkom kriminalu Saveta Evrope. Na osnovu toga, u hrvatsko zakonodavstvo uvedena su nova krivična dela, dok su neka postojeća izmenjena i osavremenjena: dečja pornografija na računarskom sistemu ili mreži (član 197 KZ Hrvatske); povreda tajnosti, celovitosti i dostupnosti računarskih podataka, programa i sistema (čl. 223); računarsko krivotvorenje (čl. 223a); računarska prevara (čl. 224a) i rasna i druga diskriminacija (čl. 174)[32]. Na osnovu analize pomenutih dela, može se reći da je hrvatski zakonopisac u potpunosti preuzeo obaveze koje se tiču implementacije Konvencije Saveta Evrope, kao i Dodatnog protokola uz Konvenciju.

30 Izvor: Nate Anderson, *World's Worst Internet Law*, http://arstechnica.com/news.ars/post/2006-0804-7421.html, 03.10.2007

31 Internet je izvor ogromnog broja istraživanja nacionalnih zakonodavstava i međunarodnih organizacija o visokotehnološkom kriminalu. Pogledati npr. http://www.legi-internet.ro/en/laws.htm, 03.10.2007. (ova internet stranica sadrži linkove prema svim važnijim odlukama međunarodnih organizacijama koje su na neki način povezane sa savremenim tehnologijama – posebno kada je reč o odlukama Evropske unije); http://www.interpol.int/Public/TechnologyCrime/default.asp, 03.10. 2007. (deo internet prezentacije Interpola posvećen visokotehnološkom kriminalu); http://www.mcconnellinternational.com/services/ Updatedlaws.htm, 03.10.2007. (linkovi ka najnovijim izmenama nacionalnih zakona pojedinih država); http://www.mosstingrett.no/info/legal.html, 03.10.2007. (verovatno najpotpuniji pregled nacionalnih zakonodavstava, kada je reč o ovoj oblasti prava).

32 Ovde se radi o postojećem krivičnom delu koje je dopunjeno u skladu s Dodatnim protokolom uz Konvenciju o visokotehnološkom kriminalu, koji je Hrvatska potpisala ali ga nije ratifikovala.

Ipak, Hrvatska još nema poseban zakonski akt o ovoj vrsti kriminala, kao ni specijalizovane organe u tužilaštvu i sudstvu. Pri policiji postoji posebna jedinica koja se bavi visokotehnološkim kriminalom kao delom svoje nadležnosti u borbi protiv piraterije. Ova jedinica je postigla zapažene rezultate poslednjih godina i deo je veće mreže regionalne saradnje za suzbijanje sajber-kriminala.

Italija je inkriminisala tri krivična dela koja se tiču visokotehnološkog kriminala: neautorizovan pristup računaru ili telekomunikacionoj mreži; nezakonit posed i distribuciju pristupne šifre računaru ili telekomunikacionoj mreži i distribuciju programa napravljenih sa ciljem da se ošteti ili ugrozi računarski sistem.[33] Slična je situacija i u *Sloveniji*, koja je uz Albaniju jedina od država centralne i istočne Evrope koje su ratifikovale i Konvenciju o visokotehnološkom kriminalu i Dodatni protokol uz Konvenciju.

Australija je 2001. donela Zakon o visokotehnološkom kriminalu, kojim je izmenila postojeći Krivični zakon i inkriminisala dela neovlašćenog pristupa ili menjanja računarskih podataka (član 478.1). *Francuska* je ovu grupu dela uvela u Krivični zakonik još 1993. godine, pa otuda poglavlje nosi naziv Napad na sisteme za automatsku obradu podataka (članovi 323–1 do 323–4). Visokotehnološki kriminal je prisutan isključivo u krivičnim zakonima (zakonicima) *Švedske, Nemačke, Holandije, Švajcarske, Norveške, Poljske, Španije,* dok su posebne zakone koji se bave ovim delima doneli, između ostalih, *Ujedinjeno Kraljevstvo, Indija, Izrael, Japan, Portugal, SAD.*[34] Pojedine zemlje još ne poznaju nikakve oblike sankcionisanja štetnog ponašanja na računarskim mrežama, ali su već postale izuzetak (*Argentina, Tunis*).

7. PERSPEKTIVE RAZVOJA VISOKOTEHNOLOŠKOG KRIMINALA I SISTEMA ZA NJEGOVO SUZBIJANJE

Ova kratka studija ima pre svega za cilj da ukaže na osnovne pravce dosadašnjeg razvoja visokotehnološkog kriminala, ali i tendencije da on doživi ekspanziju geometrijskom progresijom, koja je već započela u mnogim zemljama sveta. Kako se pravnim sredstvima može suzbiti ovaj oblik kriminaliteta?

Pre svega, treba ojačati nacionalno zakonodavstvo. Procesni problemi, a naročito neupućenost većine učesnika postupka u ciljeve, sredstva i način funkcionisanja kriminalaca i organizovanih kriminalnih grupa koje vrše ovakva dela, po pravilu, imaju dvostruku štetu: s jedne strane, velika je verovatnoća da će okrivljeni biti oslobođeni zbog nesposobnosti onih institucija koje su nadležne za njihovo gonjenje i kažnjavanje; s druge strane, takav ishod prozvodi kontraefekat, pa se u pojedinim slučajevima krše prava građana da bi se po svaku cenu došlo do osuđujuće presude.

33 Krivični zakon Italije, članovi 615-ter, 615-quter i 615-quinquies.

34 Više o zakonodavstvu SAD koje se tiče sajber-kriminala na internet adresama: http://www.cybercrime.gov, http://www.dc3.mil/dc3/home.htm, 03.10.2007

Potom, treba postati svestan da nijedna država na svetu nije usamljena u ovom problemu. Sajber-kriminal je globalna pojava, „globalnija" od bilo kog do sada poznatog oblika kriminaliteta. Praktično za nekoliko sekundi možete izvršiti krivično delo u Indiji, sedeći za računarom u Švedskoj. Samo poimanje takvog potencijala zloupotrebe savremenih tehnologija nameće logičan zaključak: da bi se ovakav kriminalitet sprečio, potrebna je izuzetno živa i sveobuhvatna saradnja među državama. Ali, treba otići i korak dalje – ova saradnja je potrebna i na mnogo operativnijem, efikasnijem nivou, između policija zemalja, različitih organizacija koje se bave sigurnošću interneta i računarskih mreža uopšte, između internet provajdera i svih ostalih koji mogu pružiti korisne podatke o postojanju nekog oblika kriminaliteta na nekoj računarskoj mreži.[35]

Ovakav način razmišljanja nas dovodi i do drugog elementa koji je veoma bitan za saradnju: međunarodne konvencije, koja bi na adekvatan način obradila i materijalne i procesne probleme u oblasti sajber-kriminala. Da li Konvencija Saveta Evrope predstavlja dokument koji je dorastao zadatku ujedinjenja svih država i organizacija sveta u borbi protiv modernih zločinaca? Na ovo pitanje je teško dati eksplicitan odgovor, ali je činjenica da države previše oklevaju da je ratifikuju i usaglase nacionalna zakonodavstva s njenim tekstom. Budući da je prošlo nekoliko godina od njenog donošenja, da je donet i Protokol, da se u međuvremenu visokotehnološki kriminal dodatno razvio, da je u pitanju akt donet pod okriljem regionalne a ne globalne organizacije, možda bi trebalo razmišljati u pravcu donošenja nove konvencije u okviru Ujedinjenih nacija ili neke od specijalizovanih agencija.

Da li je takva reakcija možda nepotrebna? Da li je opasnost od visokotehnološkog kriminala preuveličana? Iako ovaj tekst nudi više pitanja nego odgovora, konstatacija nego saveta i preporuka, što već dovoljno svedoči o tome kakva je nepoznanica *cybercrime*, jedno se sa sigurnošću može konstatovati: osnovna prepreka njegovoj daljoj ekspanziji jeste činjenica da ogroman broj ljudi širom sveta i dalje nema pristup savremenim tehnologijama, niti dovoljan životni standard da počne da ih koristi u svakodnevnom radu ili zabavi. Kako se ove tehnologije budu širile, pre svega na zemlje Afrike i Azije, otvoriće se nova „tržišta" za sajber-kriminalce i posledice ove vrste kriminaliteta će premašiti, i po zaradi počinilaca i po broju oštećenih, neke od oblika klasičnog organizovanog kriminala. Visokotehnološki kriminal se sastoji od nekoliko potpuno različitih oblika nedozvoljenog ponašanja. Za sada prednjače „piraterija" i internet prevare. Daljim razvojem komunikacija i organizovanjem kriminalaca koji svoje zločine obavljaju za tastaturom, povećaće se i broj potencijalnih žrtava, ali i načini na koji se one mogu oštetiti. Zato je edukacija građana, uz međunarodnu saradnju, strože nacionalno zakonodavstvo i edukaciju ljudi koji istražuju i procesuiraju ovakve slučajeve, jedan od osnovnih elemenata buduće zaštite i prevencije sajber-kriminala.

35 Uključujući i „obične" korisnike računara i računarskih mreža, koji se svakodnevno susreću s različitim oblicima nedozvoljenog ponašanja nepoznatih lica. Ovaj bazični nivo percepcije krivičnog dela je od izuzetnog značaja za istražne organe, koji na taj način iz neposrednih izvora dobijaju korisne i upotrebljive informacije.

Mario Reljanović, MA
Institute of Comparative Law
Belgrade

CYBER-CRIME – THE NOTION, LEGAL REGULATIONS AND EXPERIENCES

Commercialization of computer technologies and their large usage in both business and private purposes, as well as more and more developed systems of communication between people caused the occurrence of new type of unlawfull behavior – called cybercrime. Cybercrime has lots of common points with pre-existing sorts of criminal behavior, but also has its specific elements, which this paper tries to point out. Deprived of intention to offer definitive and final answers, author refers to comparative practice and its problems, marking possible ways of their future solution. Finally, analysis of most important international documents and national legislation of several specific countries reveals what changes are to be expected in this field of law in years to come. Materials gathered in such way may be used as a road sign to further acting considering cybercrime in Serbia.