Dr Dragan Prlja
Mr Mario Reljanović
Institut za uporedno pravo, Beograd Primljeno: 01.10.2009.

VISOKOTEHNOLOŠKI KRIMINAL – UPOREDNA ISKUSTVA

Visokotehnološki kriminal se naglo razvio u poslednjoj deceniji XX veka, a u XXI veku njegova evolucija je još evidentnija. Države su odgovorile uvođenjem novih mera u svoja krivična zakonodavstva, pokušavajući da pomire tradicionalno krivično pravo sa zahtevima za percipiranjem, istraživanjem i dokazivanjem novih krivičnih dela. Nakon prvog perioda implementacije ovih mera, može se govoriti o relativnom uspehu, ali se isto tako mora ukazati i na nedostatke shvatanja koja trenutno prevladavaju u ovoj oblasti. Unifikacija i harmonizacija, kao i efikasna međunarodna saradnja, osnovne su pretpostavke za bolju koordinaciju nadnacionalnih napora za suzbijanje ove vrste krivičnih dela. Komparativna analiza nije moguća bez osvrta na jedini relevantni međunarodni instrument na polju visokotehnološkog kriminala – Konvenciju o visokotehnološkom kriminalu Saveta Evrope i ukazivanja na njen značaj u globalnim okvirima. Najzad, treba se ukratko osvrnuti i na postignuto u Srbiji, koja je jedna od država koje su na vreme uvidele potrebu za specijalizacijom državnih organa i postavljanjem visokih standarda implementacije savremenih pravno-tehničkih instrumenata za borbu protiv zloupotrebe visokih tehnologija.

Ključne reči: visokotehnološki kriminal, krivično pravo, privatnost, elektronski dokazi, uporedno pravo.

1. Zakonski izrazi vezani za dela visokotehnološkog kriminala

Dela visokotehnološkog kriminala (u daljem tekstu: VTK) se nužno razlikuju od tzv. „klasičnih“ krivičnih dela, i to iz više razloga. Najpre, ona neminovno u gotovo svakom slučaju poseduju element inostranosti; drugo, u samom delu VTK je često inkorporirano još neko krivično delo,

koje se može izvršiti i na klasičan način – npr. prevara, falsifikovanje i sl; konačno, ova dela pretpostavljaju korišćenje novih, elektronskih tehnologija za njihovo izvršenje. Otuda je reakcija zakonodavaca u zemljama koje su ovu grupu krivičnih dela inkriminisale išla u pravcu definisanja putem uvođenja niza novih pojmova, do tada nepoznatih nacionalnim pravnim sistemima.

Ukoliko se analiziraju različita zakonodavstva, može se zaključiti da je terminologija slična, ali da ne postoji stoprocentna harmonizovanost. Krivični zakonik Srbije objašnjava sledeće termine, koji se koriste u zakonskom tekstu:

... "*Računarskim podatkom* se smatra predstavljena informacija, znanje, činjenica, koncept ili naredba koji se unosi, obrađuje ili pamti ili je unet, obrađen ili zapamćen u računaru ili računarskoj mreži.

Računarskom mrežom smatra se skup međusobno povezanih računara koji komuniciraju razmenjujući podatke.

Računarskim programom smatra se uređeni skup naredbi koji služe za upravljanje radom računara, kao i za rešavanje određenog zadatka pomoću računara.

Računarski virus je računarski program ili neki drugi skup naredbi unet u računar ili računarsku mrežu koji je napravljen da sam sebe umnožava i deluje na druge programe ili podatke u računaru ili računarskoj mreži dodavanjem tog programa ili skupa naredbi jednom ili više računarskih programa ili podataka." [1]

Ukoliko se pogledaju uporedna rešenja, može se doći do zaključka da je ovaj pristup gotovo opšteprihvaćen – navedeni termini se doista koriste kao osnova za inkriminisanje dela VTK u različitim zakonodavstvima. Međutim, Evropska konvencija o visokotehnološkom kriminalu sadrži unekoliko različite definicije pojmova:

... "a) „računarski sistem" označava svaki uređaj ili grupu međusobno povezanih ili zavisnih uređaja, od kojih jedan ili više njih, na osnovu programa, vrši automatsku obradu podataka;

b) „računarski podatak" označava svako predstavljanje činjenica, informacija ili koncepata u obliku koji je podesan za njihovu obradu u računarskom sistemu, uključujući i odgovarajući program na osnovu koga računarski sistem obavlja svoju funkciju;

---

[1] Član 112, stavovi 17-20. Krivičnog zakonika, Sl.glasnik RS 85/05, 72/09.

v) „davalac usluge" označava:

i. svaki javni ili privatni subjekt koji korisnicima svoje usluge pruža mogućnost komuniciranja preko računarskog sistema, i

ii. svaki drugi subjekt koji obrađuje ili čuva računarske podatke u ime takve komunikacione usluge ili korisnika takve usluge.

g) „podatak o saobraćaju" označava svaki računarski podatak koji se odnosi na komunikaciju preko računarskog sistema, proizvedenu od računarskog sistema koji je deo lanca komunikacije, a u kojoj su sadržani podaci o poreklu, odredištu, putanji, vremenu, datumu, veličini, trajanju ili vrsti predmetne usluge." [2]

Ostala zakonodavstva imaju gotovo identična rešenja srpskom primeru koji smo naveli. Osnovni pojmovi koji se javljaju u zakonskom tekstu su: računar, računarski podatak, računarski sistem, računarski saobraćaj.[3] Ove definicije, kao i inkriminacije dela VTK su po pravilu smeštena u krivičnim zakonima zemalja, eventualno i u posebnim zakonima koji se bave isključivo ovom vrstom kriminaliteta. Tako, Austrijski Krivični zakonik u članu 74. daje definicije najvažnijih pojmova. Među njima je i definicija kompjuterskog (računarskog) sistema kao "jednog ili više kombinovanih uređaja koji služe automatskoj obradi podataka". Isti član upozorava da je pojam kompjuterskog programa istovetan pojmu podatka, u smislu tog Zakona. Član 6. poglavlja III Finskog Krivičnog zakona pod podacima podrazumeva "svaki dokument, ... audio i video snimak, kao i svaki drugi snimak koji se može obraditi"... Svaki takav podatak se može koristiti i kao dokazno sredstvo u krivičnom postupku. Zakon 161/2003 Rumunije u članu 35. daje precizne definicije "računarskog sistema", "automatske obrade podataka", "računarskog podatka", "računarskog programa", "provajdera usluga", "podatka o saobraćaju", "podatka o korisniku"," merama bezbednosti" i "pornografskog materijala sa maloletnim licem". Italijansko zakonodavstvo je nešto siromašnije – postoje definicije "računarskog dokumenta (podatka)" i "podatka o saobraćaju". U mnogim zakonodavstvima koja ne sadrže posebne definicije, kao što je npr. litvansko, ova praznina popunjena je ratifikacijom Konvencije o visokotehnološkom kriminalu, čije se definicije u praksi direktno primenjuju.

---

[2] Član 1 Konvencije o visokotehnološkom kriminalu, Sl. glasnik RS 19/09.

[3] Npr. u zakonodavstvima Francuske, Nemačke, Portugala, Kipra, itd.

2. Privatnost u cyberspace-u

Privatnost ličnosti je priznata kao osnovno ljudsko pravo. Privatnost, sa stanovišta svake države, ima svoju aktivnu i pasivnu stranu – ona se mora uzdržavati od postupaka koji bi narušili privatan život pojedinca, odnosno privatnost porodice, a sa druge strane moraju se u svakom trenutku obezbediti uslovi da takva privatnost ne bude narušena od strane nekog trećeg lica. Dakle, država se uzdržava od pojedinih postupaka, istovremeno inkriminišući takve i slične nedozvoljene postupke drugih lica.

U sferi visokih tehnologija, privatnost dobija nove dimenzije. Osnovni konflikt koji se pokušava razrešiti odnosi se na očuvanje privatnosti korisnika interneta, u situaciji kada ona može biti ugrožena na najrazličitije načine. "U cilju… povećanja sloboda izražavanja informacija i ideja, države-članice treba da poštuju volju korisnika (interneta, *prim.aut.*) da ne otkriju svoj identitet."[4] Sloboda mišljenja i sloboda izražavanja, pravo na privatnost, ličan i porodičan život – sva ova prava se prepliću i može se slobodno reći da se istovremeno i ugrožavaju kroz opasnosti koje prete korisnicima računara i mobilnih telefona, kao i ostalih uređaja i vidova komunikacije putem savremenih tehnologija. Od mnogobrojnih načina na koje se mogu prekršiti ili neopravdano ograničiti, tri problema čija detaljnija analiza sledi, svakako su najčešći.

2.1 Upotreba visokih tehnologija za prisluškivanje komunikacija

Pravo na privatnost je dvostruko ugroženo, kada je reč o prisluškivanju komunikacija putem visokih tehnologija. Najpre, tu je potreba državnih institucija da brane javni poredak, kao i ljudska prava građana. Da bi to ostvarili, nužno je dati im određena ovlašćenja, prema kojima će u specifičnim situacijama moći da krše prava pojedinca za koga se smatra da je počinilac krivičnog dela. Sa druge strane, postoje nebrojeni načini kako jedan pojedinac može zloupotrebom savremenih tehnologija ugroziti pravo na privatnost drugog pojedinca, ili grupe ljudi.

Da bi državni organi, po pravilu policija i organi pravosuđa, mogli da delaju u ovoj osetljivoj oblasti, potrebno je ustanoviti određene standarde, kako svoja ovlašćenja ne bi prekoračili i kako se zaštita ne bi pretvorila u još jedan način ograničavanja ljudskih prava pojedinaca. Na osnovu prak-

---

[4] Deklaracija Komiteta ministara Saveta Evrope o slobodi komunikacije na internetu od 18. maja 2003. godine.

se Evropskog suda za ljudska prava, J.Dempsey je izveo osnovne principe postupanja državnih organa prilikom presretanja komunikacija, koji su vezani za upotrebu novih tehnologija:

- standardi za presretanje podataka moraju se jasno odrediti zakonom, dovoljno precizno kako bi se sprečila svaka njihova arbitrerna primena;
- dozvola (odobrenje) za presretanje mora biti izdata od strane nezavisnog organa (najbolje od strane sudije);
- presretanje podataka se može vršiti samo u okviru istražnih radnji o teškim krivičnim delima;
- presretanje podataka se može vršiti samo ako postoje čvrsti dokazi da je prisluškivano lice umešano u kriminalne aktivnosti;
- presretanje podataka se može vršiti samo kada ostale tehnike koje manje ugrožavaju privatnost ličnosti nisu dovoljne;
- svako odobrenje za prisluškivanje mora se odnositi samo na određenu osobu ili događaj;
- pravila o prisluškivanju moraju se odnositi podjednako na sve komunikacije između dva lica, bez obzira da li uključuju glas, faks, slike ili podatke, žičnu ili bežičnu, digitalnu ili analognu komunikaciju;
- domašaj i vremensko trajanje prisluškivanja moraju biti ograničeni;
- prisluškivanje se mora vršiti na način koji najmanje urušava privatnost lica, a da se pri tome mogu prikupiti potrebni dokazi;
- informacije koje su prikupljene ili presretnute na ovaj način, mogu se koristiti samo u svrhe za koje se prisluškivanje vršilo, ili za svrhu nacionalne bezbednosti;
- sudija koji je odobrio prisluškivanje mora dobiti povratne informacije o njegovom sprovođenju;
- sva prisluškivana lica u okviru istražnih radnji o krivičnom delu se nakon završetka prisluškivanja moraju obavestiti o tome, bez obzira da li je protiv njih podignuta optužnica;
- moraju se omogućiti mehanizmi za naknadu štete, ukoliko dođe do kršenja standarda o poštovanju privatnosti lica.[5]

---

[5] Jim Dempsey, *Protecting Privacy and Freedom of Communication in the Fight against Cybercrime*, Southeast Europe Cybersecurity Conference, Sofija, Bugarska, 8-9. septembar 2003.

Ovi standardi naravno nisu formalizovani kroz neki nacionalni ili međunarodni pravni instrument koji bi bi oobavezan za države; ipak, oni jasno određuju put kojim se države moraju kretati da bi njihovo delovanje ostalo u granicama prihvatljivim za demokratsko društvo. U Smernicama za saradnju između organa za sprovođenje zakona i internet provajdera u borbi protiv visokotehnološkog kriminala, koje je objavio Savet Evrope 2008. godine[6], internet provajderi i policijsko-tužilački istražni organi su označeni kao osnova na kojoj počiva sistem za otkrivanje i istraživanje ove vrste krivičnih dela. Za svaku državu je važno da njihov odnos reguliše na način koji bi omogućio nadzor nad saobraćajem na internetu, ali istovremeno garantovao zaštitu svih prava korisnika računara. Smernice izričito preporučuju da se svaki nalog koji potiče od tužilaštva ili policije može dostaviti isključivo u pisanom obliku, a u ekstremno hitnim slučajevima kada je moguć samo usmeni dogovor, dokumentacija mora biti naknadno dostavljena bez odlaganja. Zahtevi moraju biti jasni i nedvosmisleni, odnosno precizni i usmereni samo na one podatke koji su nužno neophodni radi sprovođenja istražnih radnji. Takođe, svi podaci ove vrste moraju biti poverljivi i upotrebljavati se samo za svrhe zbog kojih su prikupljeni.[7]

Prisluškivanje komunikacija i presretanje podataka u istrazi policije i tužilaštva je u uporednom zakonodavstvu rešeno sa izuzetnom pažnjom, poštujući najviše standarde ljudskih prava, a posebno prava na privatnost i na izražavanje mišljenja.[8] Po pravilu, za prisluškivanje i presretanje komunikacije su zaduženi isključivo specijalizovani policijski organi, a njima su potrebni odobrenje suda i/ili naredba tužioca da mogu pristupiti iz-

---

[6] *Guidelines for the cooperation between law inforcement and internet service providers against cybercrime*; dokument je usvojen na globalnoj konferenciji o saradnji protiv visokotehnološkog kriminala u organizaciji Generalnog direktorata za ljudska prava i pravne poslove Saveta Evrope, 1. i 2. aprila 2008. godine. Internet izvori: http://www.coe.int/t/DGHL/cooperation/economiccrime/cybercrime/cy_activity_Interface2008/567_prov-d-guidelines_provisional2_3April2008_en.pdf i http://www.ifap.ru/library/book294.pdf, 20.10.2009.

[7] *Ibidem*, tačke 25-28. i 32.

[8] Podaci korišćeni u analizi objavljeni su u izveštaju RAND korporacije, sačinjenog za Evropsku komisiju: Lorenzo Valeri *et alia*, *Handbook of Legal Procedures of Computer and Network Misuse in EU* Countries, Cambridge, 2006; takođe, korišćeni su podaci iz nacionalnih izveštaja država Savetu Evrope, koji se mogu naći na internet adresi http://www.coe.int/cybercrime, 20.10.2009.

vršenju te vrste istražnih radnji. Npr. u Finskoj odobrenje za prisluškivanje i presretanje komunikacije izdaje isključivo viši sud, i to samo za dela koja su taksativno navedena kao teža krivična dela (u toj grupi se nalaze i dela VTK). U Francuskoj je prikupljanje elektronskih dokaza regulisano Zakonom o krivičnom postupku; presretanje i prisluškivanje komunikacija dozvoljeno je samo za krivična dela za koja je propisana minimalna kazna zatvora od dve godine, i to ako se do dokaza ne može doći na drugi način a imaju poseban značaj u postupku (član 100. Zakona o krivičnom postupku). U Belgiji nalog za presretanje i prisluškivanje izdaje tužilac. Nemačka je na zanimljiv način rešila prazninu u svom zakonodavstvu: pravila o pretresu stana, odnosno zgrade analogno se primenjuju i na „pretres" putem internet konekcije ili u sklopu neke druge računarske mreže, kao i na pretraživanje sadržaja na pojedinačnom računaru. Ovo znači da je u svakom slučaju potreban nalog izdat od sudije, ili tužioca u izuzetnim (hitnim) slučajevima. Ista pravila važe i kada je reč o presretanju elektronskih komunikacija, ali je ovde pridodat i uslov da krivično delo koje se istražuje mora pripadati naročito teškim delima koja su taksativno navedena u Zakonu o krivičnom postupku. Ista je situacija i u Poljskoj – presretanje podataka i prisluškivanje elektronskih komunikacija moguće samo za dela koja su izričito navedena u Zakonu o policiji ili Zakonu o krivičnom postupku.

Priča o presretanju podataka ima i drugu stranu. Jedno lice može na više načina doći do sadržine komunikacije drugog lica, korišćenjem ilegalnog hardvera ili softvera. Ovakvo ponašanje je u mnogim državama određeno kao kažnjivo[9], ali za sada ni zakonodavstvo ni praksa nisu ujednačeni. Najjednostavniji način za ulazak u tuđ računar jeste saznavanje njegove lozinke, kao i lozinke za korišćenje elektronske pošte. U vezi sa time, još uvek se vodi velika polemika čiji su podaci koje zaposleni drži na računaru preduzeća u kome radi. Ovi podaci se mogu ticati poslovne komunikacije, planova, dokumenata i sl, ali se ulaskom u računar zaposlenog može doći i do njegovih privatnih podataka, koje on neminovno ostavlja pretraživanjem interneta, posetama socijalnim sajtovima, forumima, pristupanjem privatnom nalogu elektronske pošte, i sl. Počev od

---

[9] Videti npr. Krivični zakonik SAD – Title 18, Chapter 119 „*WIRE AND ELECTRONIC COMMUNICATIONS INTERCEPTION AND INTERCEPTION OF ORAL COMMUNICATIONS"*, dostupno na internet adresi: http://www.law.cornell.edu/uscode/18/usc_sup_01_18_10_I_20_119.html, 20.10.2009.

banalnih primera, kada novi korisnik nekog računara može pristupiti svim onim nalozima koje je koristio prethodnih zato što je računar automatski memorisao pristupne šifre ili je prethodni korisnik jednostavno ostao "ulogovan" u određeni privatni sadržaj, pa sve do "nasilnih" upada u računare od strane poslodavca[10], članova porodice ili osoba bliskih korisniku, stvara se sivo područje prava koje za sada nije uniformno rešeno. Sa druge strane, postoje "presretači" komunikacije preko mobilnih telefona. Ovi uređaji su u mnogim državama legalni, uključujući i Srbiju. Ovo je slučaj pre svega zato što zakonodavstvo ne može da isprati sve tehnološke novitete koji se pojavljuju na tržištu. Uređaji o kojima je reč narušavaju na očigledan način privatnost ličnosti – jedni "sakupljaju" razgovore i poruke poslate sa mobilnih telefona osoba koje su u neposrednoj blizini onoga ko poseduje uređaj. Drugi "uređaji" su zapravo softveri koji se instaliraju na telefone prisluškivanih osoba. Ovi softveri šalju podatke o svim aktivnostima koje vlasnik ima na telefonu, a u zavisnosti od njihovog podešavanja, mogu i direktno prenositi sve razgovore vlasnika telefona. Očigledno je da ovakva oprema ne može biti legalna, ali je to još jedan od problema koji su specifični za razvoj VTK – zakonodavci po pravilu zaostaju za maštom počinilaca i inovatora.

2.2 Kopiranje i zaplena privatnih podataka

Ove radnje ugrožavanja privatnosti se pre svega odnose na zaplenu računara ili kopiranje hard diskova od strane istražnih organa u pretkrivičnom postupku. Naime, u svim državama u kojima je izvođenje elektronskih dokaza posebno regulisano, ili je uobičajeno pred sudovima koji ih prihvataju po analogiji, standard je da se podaci kopiraju, a ne fizički plene. Ovo je naročito korisno kada se podaci nalaze na serverima (npr. prilikom postavljanja internet sajtova koji imaju zabranjenu sadržinu), čija je zaplena praktično nemoguća bez stvaranja velike štete provajderima usluga. Naravno, postoje različite situacije i ponekada će biti korisnije da se računar, odnosno nosač relevantnog podatka, fizički odvoji od sistema – npr. kada je u pitanju nosilac virusa. Kao što se može videti, ove radnje

---

[10] Pitanje je da li je upad u računar koji koristi zaposleni sam po sebi nedozvoljen. Neke od odgovora daje studija o ponašanju poslodavaca i zaposlenih u SAD: *Employee Privacy and Statutory Individual Rights*, u: Karen E. Ford, Kerry E. Notestine, Richard N. Hill (ur.), *Fundamentals of Emplyment Law*, American Bar Association, 2000.

će vrlo često pretpostavljati uzurpiranje privatnosti i trećih lica, kao što su internet provajderi. Otuda se zapleni i kopiranju podataka prilikom vršenja istražnih radnji posvećuje posebna pažnja u nacionalnim zakonodavstvima. Može se reći da su standardi koje su države uspostavile gotovo istovetni. Najpre, ove radnje se mogu vršiti samo po nalogu suda ili tužioca – policija uglavnom nema ovlašćenja da ih samostalno sprovodi[11]; potom, kao garantija minimuma narušavanja privatnosti se postavljaju određeni pravni standardi – sakupljaju se samo podaci koji su relevantni, takvi podaci su poverljivi i ne mogu se upotrebiti van određenog istražnog ili sudskog postupka; uvek će se primeniti ona mera koja će načiniti najmanje štete vlasniku i korisniku podataka, kako u materijalnom smislu tako i u smislu izlaganja privatnih podataka javnosti.

Austrijski zakon o krivičnom postupku (članovi 143.-149.) postavlja jasan standard kada je reč o zapleni i kopiranju podataka – uvek će se primeniti ona mera koja je najmanje intruzivna i koja će načiniti najmanju štetu, kako okrivljenom tako i trećim licima. Takođe, predmet kopiranja ili zaplene su samo oni podaci koji su relevantni za istragu ili krivični postupak.[12] Internet provajderi su obavezni da sačuvaju i proslede sve podatke za koje sumnjaju da mogu predstavljati dokaz o izvršenju krivičnog dela (ista zakonska obaveza postoji i u Danskoj). U Belgiji, isto kao i kod presretanja i prisluškivanja komunikacija, nalog izdaje tužilac. On ima dosta veliku slobodu u odlučivanju da li će podaci biti zaplenjeni ili kopirani, a postoji i mogućnost njihovog uništenja ukoliko je realna opasnost da će se dalje širiti a ne mogu se onesposobiti (npr. računarski virusi). Podaci koji se prikupe na ovaj način su poverljivi – oni se mogu koristiti samo u svrhe istrage, odnosno krivičnog postupka, a vlasnik podataka, odnosno administrator sistema sa koga su uklonjeni, zaplenjeni ili kopirani, mora biti obavešten o kojim se podacima radi. Na Kipru, u sudskom postupku će biti predstavljeni podaci na onaj način koji sud bude smatrao zadovoljavajućim. Ako se ne mogu predstaviti u materijalnom obliku, sud će tražiti mišljenje veštaka. U Estoniji nalog za zaplenu ili kopiranje podataka mogu dati i sud i tužilac; podaci će biti zaplenjeni samo ukoliko njihovo kopiranje nije moguće.

---

[11] Izuzetak je npr. Češka.

[12] Slične formulacije se mogu naći i u zakonima Estonije i Španije.

2.3 Krađa lika i identiteta i drugi vidovi (ne)zakonitog ponašanja

Krađa identiteta (eng. *phishing*) znači preuzimanje "uloge" nekog lica na internetu, redovno u cilju sticanja neke materijalne ili druge koristi. Ovo je najdrastičniji atak na privatnost ličnosti, jer se počinilac, nakon što je prevarom ili na drugi način došao do vitalnih podataka za preuzimanje nečijeg identiteta (internet i druge šifre, brojevi platnih kartica, i sl.) predstavlja u njegovo ime, zaključuje poslove ili ostvaruje društvene kontakte.[13] U tom smislu, krađa identiteta pretpostavlja prethodno izvršenje nekog drugog krivičnog dela (prevare, upada u tuđi računar ili računarski sistem, postavljanje virusa ili drugog štetnog softvera). Postoje međutim i drugi načini intruzije u privatan život ljudi, koji se mogu okarakterisati kao "manje ili više kažnjivi". Neki od njih su zaista inkriminisani; o nekima zakoni ćute i kao takvi predstavljaju samo moralno neprihvatljivo ponašanje:

• *Korišćenje tuđih (javnih) podataka*. Ovde nije reč o preuzimanju identiteta neke osobe radi ostvarivanja koristi, već o jednostavnom korišćenju javno dostupnih podataka radi stvaranja fiktivnog lica koje se pojavljuje na internetu, npr. na forumima, socijalnim sajtovima, sajtovima za četovanje i upoznavanje, i sl. Ova aktivnost se svodi na razmenu tuđih slika, rezimea, stavova, koje je osoba pronašla na internetu, kako bi se lakše upoznala sa nekom trećom osobom ili ostvarila cilj socijalizacije na neki drugi način. Iako se svakako može okarakterisati kao nemoralna, ova vrsta aktivnosti (za sada) nije kažnjiva niti u jednoj državi – osim ukoliko se ne radi o silovatelju ili pedofilu, koji na taj način pokušava da pronađe svoju žrtvu, ali je i tada reč o drugim krivičnim delima a korišćenje tuđih podataka se javlja samo kao jedno od prethodnih sredstava pripreme za izvršenje.

• *Korišćenje elektronskih podataka o aktivnosti lica*. Zakoni o zaštiti podataka o ličnosti, koji su standard u pravnim sistemima razvijenih zemalja, jasno određuju kako određeni podaci do kojih dođu različite institucije, organi i drugi subjekti, mogu biti upotrebljeni. Međutim, kao i kod sledećeg primera ustupanja podataka o elektronskim adresama, moguća je zloupotreba prikupljenih podataka o jednom licu. Korišćenjem platne kartice kao sredstva plaćanja, može se npr. jasno videti šta je jedna oso-

---

[13] Ne treba zaboraviti, može i da vrši krivična dela na ovaj način, prikriven iza tuđeg identiteta.

ba kupila, u koje vreme i na kom mestu. Ako neko redovno kupuje određenu vrstu proizvoda, ili koristi neke usluge, može se (neprijatno) iznenaditi – na njegovu kućnu adresu će stići reklamni materijal odgovarajuće sadržine. Ako npr. redovno kupuje hranu za mačke, dobiće ponude za kupovinu hrane za mačke, uz prateći asortiman drugih proizvoda za životinje. Ako redovno rezerviše karte za pozorište putem interneta, može dobiti ponudu za kolekciju kućnih DVD-ova slične sadržine, itd. Iako deluje bezazleno, možda čak i kao bezopasan marketinški trik, to zapravo znači da su informacije o plaćanju te osobe dostupne nekome ko ih dalje "ustupa" različitim kompanijama. Treba se zapitati: šta će se desiti ako podaci na ovakav način budu "cureli" i kod drugih kupovina, npr. prodaje *on-line* aranžmana za letovanje? Odgovor je: onda će neko ko zna vašu kućnu adresu znati i period kada će ta kuća biti prazna, dok ste vi sa porodicom na letovanju.

• *"Prodaja" e-mail adresa i spamovanje*. Postoji nebrojeno programa čija je jedina svrha slanje što većeg broja elektronskih poruka, kako na računare (putem *e-mail* servisa) tako na mobilne telefone (putem sms servisa). Ove poruke najčešće imaju reklamni karakter, ali ponekad mogu sadržati i elemente prevarnih *e-mail*-ova (tzv. "Nigerijsko pismo", i sl.) odnosno poruka kojima se otpočinje komunikacija sa licem radi konačnog cilja izvršenja prevare. Zajednički naziv za sve ove poruke je "neželjena pošta" (eng. *spam*). Druga strana *spam*-a jeste dobijanje neželjene pošte zato što je neki od sajtova ili drugih servisa kome osoba ostavi svoju važeću *e-mail* adresu (prilikom registracije, ili u nekom sličnom slučaju) ustupa – besplatno ili za određenu naknadu – spiskove tih adresa različitim kompanijama, koje zatim šalju ogroman broj (pravih ili lažnih) reklama za najrazličitije proizvode. Tu se zapravo vrši (nezakonito) filtriranje – za razliku od automatskog slanja na adrese koje možda nisu aktivne ili čak ni ne postoje, ovde se koriste samo postojeće, aktivne adrese i "obezbeđuje" se pažnja njihovog korisnika. Iako je ovakvo "ustupanje" podataka sasvim sigurno kažnjivo u većini zemalja prema propisima o zaštiti podataka o ličnosti, praktično je nemoguće utvrditi da li je i na koji način neki od sajtova ustupio nečiju *e-mail* adresu. Protiv *spam*-a su moguće različite preventivne tehničke mere – npr. automatsko filtriranje poruka pre nego što dođu do korisnika ili odbijanje poruka koje dolaze sa određenih servera koji se koriste u velikoj meri, ili isključivo, za ovakve aktivnosti. Australija je prva država koja je inkriminisala *spam*-ovanje. Irska joj se nedavno pridružila, a obzirom na trendove narastanja neželjene

pošte i na prognoze da će ona u najskorijoj budućnosti imati udeo u ukupnom *e-mail* saobraćaju preko 90%, što čini preko milijardu poruka dnevno[14], moguće je da će i druge države slediti ovaj novozapočeti trend inkriminacije.

• *Korišćenje opreme za nadzor i obezbeđenje*. Oprema koja je do pre nekoliko godina bila suviše sofisticirana i skupa za opštu upotrebu, masovnom proizvodnjom je postala dostupna velikom krugu korisnika. Iako ne spada u ono što se obično podrazumeva "visokom tehnologijom", njome se može značajno umanjiti ili čak i ukinuti pravo na privatnost ličnosti. Televizijske kuće svakodnevno koriste ove kamere koje su instalirane na lokacijama koje su nepoznate prolaznicima na ulici. Za razliku od saobraćajnih kamera, kao i kamera obezbeđenja, koje se fokusiraju na jedan segment okoline u kojoj se nalaze, i koje imaju društvenokoristan cilj i samim tim opravdanje svog postojanja, kamere do kojih se može doći i preko mnogobrojnih internet sajtova, kao i one koje se koriste u televizijskim programima, omogućavaju veće zadiranje u privatnost ljudi nego što imaju korisnu svrhu. Naravno, osobe na ulici nisu zaštićene pravom na privatnost, ali se mogu zapitati da li je moguće da neko svakodnevno prati njihovo kretanje putem ovih javnih kamera, kao i da li je moguće da snimci napravljeni ovim kamerama budu dostupni praktično svakom pojedincu koji za njih bude zainteresovan. Čak i ukoliko ovakvi snimci ne budu upotrebljeni za vršenje krivičnih dela ili drugih nedozvoljenih radnji, čini se da preovladava mišljenje da ljudi ne žele da žive "u kući velikog brata", u svetu u kome svakog trenutka postoji mogućnost da budu snimljeni i praćeni. Jedan od problematičnih aspekata ovakve situacije se jasno pokazuje i kroz kotroverzni program koji je lansirala kompanija *Google – Google Street View*, koji može pokazati slike iz različitih ulica većih gradova širom sveta. Ovaj program se zasniva na realnim slikama ulica „uživo", na kojima se nalaze ljudi, automobili i sl. Koliko se duboko na ovaj način zadire u pravo na privatnost? Možda ne najpreciznji, ali u svakom slučaju zanimljiv odgovor može ponuditi gospođa iz Velike Britanije, koja je pokrenula brakorazvodnu parnicu nakon što je slučajno na snimku jedne od ulica videla parkiran automobil svog muža ispred nepoznate kuće, u vreme kada je on navodno bio na službenom putu.[15]

---

[14] Izvor: http://www.junk-o-meter.com/stats/index.php, 20.10.2009.

[15] Izvor: Blic online, *Preko Gugla otkrila preljubu*, http://www.blic.rs/zanimljivosti.php?id=86407, 20.10.2009.

3. Kako inkorporirati specifičnosti gonjenja za dela VTK u tradicionalne krivičnopravne okvire?

Dela VTK su specifična po čitavom nizu svojih obeležja. Imajući u vidu činjenicu da se radi o relativno novoj pojavi sa izrazitim transnacionalnim obeležjima, da se radi o najraznovrsnijoj grupi krivičnih dela i kriminalitetu koji se neprestano razvija i stvara nove pojavne oblike, kao i da su države reagovale izmenama zakonodavstava tek u poslednjoj deceniji, dolazimo do niza poteškoća koje se javljaju u praksi. Sve one se mogu svesti na konstataciju da je dela VTK izuzetno teško percipirati, istraživati i procesuirati. Detaljnija analiza otkriva neke najvažnije nedostatke „tradicionalnog" krivičnog prava, kada se upotrebi bez odgovarajuće adaptacije:

• Ono što se prvo može uvideti jeste da *dela VTK imaju jasno izražen transnacionalni karakter*. Verovatno najpoznatiji primer umešanosti više međunarodnih elemenata u izvršenje jednog krivičnog dela posredstvom računara i računarskih mreža dogodio se u Austriji, prilikom akcije protiv vlasnika internet prezentacije sa dečijom pornografijom. Austrijski državljanin je postavio prezentaciju na kojoj su članovi, nakon što plate određenu sumu novca za pristup, mogli da *download*-uju različite materijale vezane za dečju pornografiju. Server na kome se prezentacija nalazila zakupljen je u Rusiji, a sam provajder je poslao 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 je posedovanje dečje pornografije u njihovim državama krivično delo, su uglavnom iz Velike Britanije i Danske. I pored komplikovanog zapleta priče, rešenje je jednostavno budući da su nadležni organi različitih država sarađivali u celom poduhvatu – vlasniku prezentacije će se suditi u Austriji, ostalim okrivljenim u zemljama čiji su državljani. Šta će se desiti kada neka od zemalja odbije da sarađuje u ovakvim istragama, iz političkih ili formalno-pravnih razloga? Kako procesuirati delo koje nije kažnjivo u državi u kojoj se nalazi počinilac, a predstavlja teško krivično delo u državi u kojoj se nalazi oštećeni? Nažalost, u takvim slučajevima sve zavisi od (ne)postojanja bilateralnog instrumenta, a najčešći rezultat će biti nemogućnost kažnjavanja počinioca. Ovakva situacija nije neobična, i ona govori o nerazvijenosti međunarodnog aspekta VTK, kao što je bio slučaj i sa mnogim drugim vrstama kriminaliteta kada su se oni pojavili na nadnacionalnom nivou, kao što su npr. te-

rorizam ili organizovani kriminal. Tokom vremena, države će uvideti potrebu da se efikasnije organizuju i njihova saradnja će sigurno jačati, a „sigurnih država" za počinioce dela VTK će biti sve manje.

• *Kako percipirati delo VTK?* Ovo je izuzetno važno pitanje, jer implicira pitanja koja bi mogla da utiču na postojeći sistem policijsko-pravosudnih organa, kao i zaštitu ljudskih prava pojedinaca. Sa jedne strane, postoji solucija konstantnog monitoringa interneta od strane policije. Ovakav vid zaštite može biti efikasan, naročito sa razvojem posebnih softvera koji su napravljeni da „uoče" ilegalna ponašanja u protoku informacija. Međutim, njihova upotreba otvara pitanje da li to znači da su svi građani koji koriste internet pod prismotrom, odnosno da se njihove komunikacije prisluškuju? Softver radi po principu (slučajnih) uzoraka i izdvaja samo one koji mogu predstavljati potencijalno krivično delo – npr. uočava delove fotografije poslate *e-mail*-om na kojima se vidi dečja pornografija; izoluje taj sadržaj i aktivira policijsku službu, koja dalje procesuira slučaj na osnovu podataka koje ima, uz pomoć internet provajdera. Na taj način se obradi delić ogromnog protoka, ali istovremeno se obradi i 99% sadržaja koji ne predstavlja nelegalnu aktivnost. Da li su na taj način oštećeni svi oni kojima se pregleda sadržaj komunikacije dok se bave poslovnim ili privatnim prepiskama, u skladu sa zakonom? Sa druge strane, bez određene reakcije nadležnih državnih organa, veći deo krivičnih dela iz ove oblasti neće biti primećen. Ponekad će se to dogoditi zato što oštećeni ni ne primeti da se desilo nešto vredno pažnje (npr. neko je preuzeo računar drugog lica i njime počinio krivično delo neovlašćenog upada u računarski sistem; vlasnik računara nije ni svestan te činjenice) ili zato što nema direktnog oštećenog koji bi mogao da se pobuni (npr. rasturanje sadržaja dečje pornografije) ili zato što oštećeni ne žele da se sazna da su bili žrtve (što je čest slučaj kod različitih internet prevara).

• *Kako biti siguran ko je počinilac krivičnog dela u pitanju?* Klasične istražne radnje, u kombinaciji sa novim specijalizovanim istražnim radnjama, po pravilu će dovesti policiju do počinioca dela VTK. To, međutim, ne mora uvek biti slučaj. Specifična priroda ovih krivičnih dela, odnosno tehnologija koje se upotrebljavaju prilikom njihovog izvršenja, naročito može doći do izražaja prilikom identifikacije *lica* koje je počinilac. Relativno lako se može doći do IP adrese sa koje je delo počinjeno, samim tim i do računara sa koga je počinjeno. Ali, da li se uvek sa 100% sigurnosti može reći ko je radio za tim računarom u vreme izvršenja krivičnog dela? Skorašnji primer iz prakse SAD je dovoljno ilustrativan. Ta-

mo je izvesni J.P. iz Ostina u Teksasu poslao mail koji je sadržao pornografsku sliku maloletnika. Kada je utvrđena IP adresa sa koje je elektronska pošta poslata, policija ga je locirala i pretresla njegovu sobu. Tom prilikom je pronašla CD sa dečjom pornografijom, i slučaj bi mogao da se smatra jednostavnim za rešavanje pred sudom, da nije postojala i druga strana priče. Naime, J.P. je stan delio sa cimerom. *E-mail* adresa je, prema korisničkom imenu, zaista upućivala na to da je cimer njen vlasnik, ali je ovaj to negirao, a nije postojala mogućnost da se zaista utvrdi ko je otvorio *e-mail* nalog. Istovremeno, pretresom nije bio uključen deo stana koji koristi cimer J.P. tako da se ne može sa sigurnošću tvrditi da li je on koristio i posedovao dečiju pornografiju. *WiFi* mreža preko koje se J.P. konektovao na internet bila je otvorenog karaktera, dakle bez zaštite i svako ko je fizički hvatao signal bežičnog interneta mogao je da ga koristi i da poseduje IP adresu koja je i dovela policiju do J.P.-a. Postojale su, dakle, dve mogućnosti: jedna da je J.P. otvorio *e-mail* nalog, koji je namerno podsećao na ime i prezime njegovog cimera, i koristeći svoju *Wi-Fi* mrežu slao slike dečije pornografije. Druga mogućnost, koja je takođe u domenu realnosti, bila je da je J.P.-ov cimer, koristeći svoj nalog i J.P.-ovu nezaštićenu mrežu, počinio ovo krivično delo. U drugom slučaju, J.P. bi svejedno bio osuđen za posedovanje dečje pornografije na CD-u koji je nađen, ali da li je cimer opravdano ostao izvan domašaja pravde? Iako je J.P. svoju odbranu zasnovao na činjenici da se otvorena *WiFi* mreža može koristiti sa bilo kog računara, sud nije imao puno razumevanja za ovu odbranu i J.P. je osuđen pred osnovnim sudom, a presudu je potvrdio nadležni apelacioni sud, na skoro pet godina zatvora. Iako je faktička procena policije i tužioca bila da nema elemenata da se goni i J.P.-ov cimer, ostaje veliko pitanje da li je samo J.P. odgovoran, kao i još šira nedoumica – kako će precedent koji je sud u ovom slučaju doneo, da otvorena *Wi-Fi* mreža nije opravdanje za njenu eventualnu zloupotrebu i korišćenje u ilegalne svrhe – dakle da uvek odgovara pretplatnik, uticati na buduću praksu?[16] Naravno, ovde se otvara još jedno pitanje na koje istražni organi trenutno nemaju odgovor, niti postoji način da će ga u skorijoj budućnosti imati: šta se dešava kada neko počini krivično delo sa laptop računara (ili bilo kog drugog mobilnog uređaja) dok je konektovan na otvore-

---

[16] Više o ovom slučaju na internet adresi: http://arstechnica.com/tech-policy/news/2007/04/child-porn-case-shows-that-an-open-wifi-network-is-no-defense.ars, 20.10.2009.

nu *WiFi* mrežu na nekom javnom mestu? Gotovo svaki aerodrom na svetu ima slobodan (besplatan) internet pristup na ovaj način, gde nikakva registracija nije potrebna. U situaciji kada se, na nekom većem aerodromu, istovremeno na mreži nalazi više stotina, pa čak i hiljada ljudi – neregistrovanih korisnika, nemoguće je utvrditi kome pripada računar sa koga je počinjena neka ilegalna radnja u *cyber* prostoru. Potpuno isto se može reći i za svaku durgu lokaciju koja ima otvorene mreže – a to je sve više slučaj sa ugostiteljskim objektima, ali i sa celim gradovima, gde lokalna samouprava finansira projekte besplatnog interneta za svoje građane.

• *Kako dokazivati delo na sudu?* Elektronski dokazi koriste se u velikom broju zemalja pred sudskim organima već duži vremenski period, ali ipak nema opšteprihvaćene definicije šta se pod elektronskim dokazima podrazumeva. U najširem smislu pod elektronskim dokazima mogu se smatrati podaci koji su skladišteni ili preneseni u digitalnoj formi koje strana u sporu koristi na sudu i to mogu biti npr. elektronska pošta, digitalne fotografije, dokumenti stvoreni u tekst procesoru ili razni drugi fajlovi stvoreni kompjuterskim programima, istorija internet pretraživanja, baze podataka, sadržaj kompjuterske memorije, kopija hard diska ili druge kompjuterske spoljne memorije, digitalni audio i video fajlovi, razne vrste logovanja, podaci sistema za globalno pozicioniranje, virusi, drugi štetni kompjuterski programi itd. Stephen Mason iz Britanskog instituta za međunarodno i uporedno pravo predložio je prošle godine sledeću definiciju: "elektronski dokazi su podaci koji su kreirani, manipulisani, skladišteni ili kojima se komunicira bilo kojim uređajem, kompjuterom ili kompjuterskim sistemom, ili su preneti preko komunikacionog sistema, a relevantni su za sudski postupak".[17] Zbog značaja pitanja elektronskih dokaza Evropska Unija realizovala je od 2005.g. do 2007.g. projekat: "Prihvatljivost elektronskih dokaza na sudu". Projekat je obuhvatio analizu zakonodavstva i sudskog postupka u šesnaest država članica Evropske Unije. Analiza zakonodavstava pokazala je da u nekim zakonodavtsvima nema definicija elektronskih dokaza dok druga sadrže takve definicije, ali one nisu najpreciznije. Zajednički zaključak je da su u svim zakonodavstvima elektronski dokazi izjednačeni sa klasičnim dokazima po svojoj snazi i to elektronski dokumenti sa papirnim dokumentima, elektronski

[17] Stephen Mason, International electronic evidence, London, British Institute of International and Comparative Law, 2008, p. XXXV.

potpis sa svojeručnim potpisom i elektronska pošta sa običnom poštom. Kada su u pitanju proceduralna pravila, kako kod građanskim, tako i u krivičnim stvarima nisu utvrđeni zajednički standardi za prikupljanje, čuvanje, i izvođenje elektronskih dokaza na sudu. Uglavnom se koriste analogije u odnosu na klasične dokaze, mada su neke zemlje kao Velika Britanija i Belgija definisale pravila za prikupljanje "kompjuterskih dokaza". Bez obzira na to koliko su precizno definisane procedure prikupljanja elektronskih podataka neophodno je svakako u tom postupku poštovati propise o zaštiti podataka i privatnosti.[18]

• *Kako edukovati poslenike u pravosuđu?* Iako na prvi pogled može da izgleda banalan, ovaj problem je zajednički za sve države, jer je za procesuiranje dela VTK potrebno zavidno predznanje o funkcionisanju savremenih tehnolgija. Jednostavno, da bi se krivično delo uopšte uočilo, a zatim i da bi se razdvojilo od „običnih" krivičnih dela, potrebno je imati dovoljno znanja o radu na računarima i drugim elektronskim tehnologijama. Potom, da bi se shvatilo šta je to opasno u ponašanju počinioca, koje su posledice njegovog dela i kako funkcioniše mehanizam njegovog izvršenja, treba posedovati naročito iskustvo o detaljnima funkcionisanja računara i računarskih mreža, kao i poznavati slične slučajeve iz prakse (nacionalne ili uporedne). Države su ove probleme uglavnom probale da reše posebnom edukacijom redovnih organa, ili uvođenjem specijalizovanih organa koji se bave isključivo delima VTK. Čini se da je drugo rešenje kvalitetnije, jer se na taj način omogućava fokusiranje tužilaca i sudija na jednu oblast prava, ali i detaljnija edukacija o tehničkim i tehnološkim aspektima, bez kojih je procesuiranje nemoguće.

• *Kako uspostaviti efikasan sistem prevencije?* Većina posmatranih država ulaže velike napore za poboljšanje svojih tehničkih i ljudskih resursa u cilju opažanja dela VTK, njihovog istraživanja, hvatanja, procesuiranja i sankcionisanja počinilaca. Mnogo manja pažnja se posvećuje edukaciji šireg kruga korisnika visokih tehnologija, kako bi se smanjila mogućnost događanja – izvršenja krivičnih dela ove vrste. Iako ovo nije krivičnopravni problem, on je indirektno vezan za još jedan nedostatak krivičnog prava: *kako sankcionisati počinioce dela VTK i kako sprečiti recidivizam*? U određenim slučajevima teških krivičnih dela, kao što su

---

[18] Fredesvinda Insa, *The Admissibility of Electronic Evidence in Court* (A.E.E.C.): *Fighting against High-Tech Crime—Results of a European Study*, Journal of Digital Forensic Practice, Volume 1, Issue 4, December 2006, str. 285 - 289.

proizvodnja i distribucija dečje pornografije, finansijske prevare većih razmera, povezanost VTK sa organizovanim kriminalom i terorizmom, zatvorske kazne su opravdane. Kod blažih slučajeva, kao što su pokušaji manjih prevara, upadi u računar ili računarski sistem bez štetnih posledica i sl, postavlja se pitanje opravdanosti zatvorskih kazni, čak i opravdanost primene krivičnih sankcije uopšte.[19] Takođe, sankcije koje su u nekim državama, naročito u SAD, izricane prethodnih godina a koje se svode na zabranu pristupa računaru počiniocu nekog krivičnog dela VTK, ne mogu više biti efikasne.[20] Posebno pitanje jeste kako se postaviti prema recidivizmu, odnosno kako ga sprečiti i kanalisati znanje takvih počinilaca (kada je reč o lakšim delima) na društvenokoristan rad, putem alternativnih sankcija i stimulisanjem kreativnosti, umesto kažnjavanja destruktivnosti.

4. Pozicioniranje država u odnosu na postavljene standarde[21]

Broj država koje su u poslednjih nekoliko godina donele specijalizovane zakone kako bi suzbile, odnosno iskorenile VTK je izuzetan. To je rezultat relanih potreba da se stane na put ekspanziji ove vrste nedozvoljenih aktivnosti. Samo u toku 2008. i 2009. godine, do trenutka završetka ovog rada, još pet država je donelo posebne zakone o visokotehnološkom kriminalu, dok čitav niz onih država koje su taj zadatak obavile ranije, sada svoje zakone redovno usaglašava sa praksom, odnosno relanošću neprekidnog razvoja ove vrste kriminaliteta.

---

[19] Poseban problem nastaje kada se kao počinilac nađe maloletno lice, ili čak lice koje je zbog svog uzrasta krivično neodgovorno. To je još jedna specifičnost ove vrste kriminaliteta: počinioci se mogu često naći među pripadnicima izuzetno mlade populacije, koji se time bave radi avanture i sticanja popularnosti u *cyber* svetu, a ne radi sticanja neke materijalne koristi.

[20] Postoji mogućnost da uskoro neće biti ni legalne. Finska je prva država koja je pristup internetu proglasila za *pravo* svakog građanina, a Ujedinjene nacije razmatraju ideju da se pravo na pristup internetu uvrsti u univerzalna ljudska prava treće generacije. Izvor: *Fast internet becomes a legal right in Finland*, http://www.cnn.com/2009/TECH/10/15/finland.internet.rights/index.html, 20.10.2009.

[21] Detaljnija analiza napora država na implementaciji Konvencije i donošenju specijalnih zakona na internet adresi: http://www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/Documents/CountryProfiles/default_en.asp, 20.10.2009.

Već je naglašeno da je osnovni dokument u evropskim, ali i svetskim okvirima u ovoj oblasti Evropska konvencija o visokotehnološkom kriminalu sačinjena 23. novembra 2001. godine u Budimpešti, pod okriljem Saveta Evrope. Zbog svog značaja, široke prihvaćenosti ali i sveobuhvatnosti, uporednu analizu treba izvršiti pre svega u smislu prihvatanja njenog sadržaja. Iako je ovaj zadatak naizgled lak, mogu se izdvojiti četiri vrste država u zavisnosti od samog odnosa prema Konvenciji: one koje su ratifikovale i implementirale Konvenciju; one koje su ratifikovale Konvenciju ali nisu sprovele mere njene implementacije; države koje nisu ratifikovale Konvenciju ali imaju razvijeno zakonodavstvo, doneto po ugledu na sadržine ovog dokumenta; države koje nisu ratifikovale Konvenciju i nemaju razvijeno zakonodavstvo u ovoj oblasti. Zaključci koje ćemo navesti biće samo sinteza posmatranja različitih država koje se mogu svrstati u jednu od ove četiri grupe.

1) *Ratifikacija i implementacija Konvencije* je u mnogim državama dovela do stvaranja posebnog sistema za praćenje, otkrivanje i procesuiranje dela VTK. Među ovim državama se nalaze Rumunija, Srbija, Mađarska, Italija, Jermenija, Finska, Nemačka, Francuska, Bugarska, itd. Mnoge od njih imaju specijalizovane organe. Uglavnom je reč o policijskim organima, ređe o pravosudnim – tužilaštvima i sudovima. Ovaj princip se pokazao kao ispravan kada je reč o efikasnosti suzbijanja VTK – specijalizovane institucije ne samo što delaju rasterećene od drugih zadataka, nego se mogu detaljnije posvetiti metodama izvršenja krivičnih dela korišćenjem visokih tehnologija, kao i izučavanju načina za njihovo sprečavanje, procesuiranje i dokazivanje na sudu.

2) Pojedine države su *Konvenciju ratifikovale, ali je nisu u potpunosti implementirale*. U ovoj grupi država mogu se pomenuti Makedonija, Kipar, Hrvatska, Velika Britanija. Njih nema puno, jer se ratifikacijom Konvencije svaka zemlja obavezuje da je, u skladu sa svojim unutrašnjim pravnim sistemom, implementira u što kraćem roku. Ipak, pojedine odredbe Konvencije u navedenim državama još uvek nisu zaživele u zakonodavstvu. Ponekad je „praznina“ u zakonodavstvu posledica specifične prakse zemalja. Tako npr. Makedonija i Kipar naizgled nemaju posebne procesne odredbe koje Konvencija sadrži, iako je materijalno pravo u potpunosti inkorporirano u njihova krivična zakonodavstva. To je pre svega zato što se na pojedine pravne institute koriste pravila „klasičnog“ prava, odnosno opšte odredbe postojećih procesnih zakona. Iako se na taj način izbegava stvaranje pravne praznine i omogućava primena Konvencije,

mora se naglasiti da ovaj način neće dugoročno dati kvalitetne rezultate. Naime, proces pribavljanja, čuvanja i korišćenja dokaza u sudskom postupku za dela VTK je jako specifičan; kao što smo već napomenuli, specifičan je zbog načina prikupljanja – dakle, samih fizičkih radnji, zbog zadiranja u privatnost ličnosti, kao i zbog specifičnog prezentovanja takvih dokaza pred sudom. Otuda klasična pravila često nisu upotrebljiva za istražne i procesne radnje koje se moraju obaviti kako bi se počinioci pronašli i kaznili. Slična je situacija i u Hrvatskoj, dok Velika Britanija ima većih problema sa implementacijom.

3) Postoje države koje, iz određenih političkih ili praktičnih razloga, *nisu ratifikovale Konvenciju ali su svoje nacionalno zakonodavstvo zasnovale na njenim rešenjima*. Mogu se odmah identifikovati dve vrste ovih država. U prvoj grupi su one kojima ratifikacija ne bi gotovo ništa značila, jer ni geografski ni politički ne pripadaju Savetu Evrope – to je npr. slučaj sa Indonezijom i Dominikanskom Republikom. Sa druge strane, tu su države koje definitivno imaju interes da načine takav korak, ali se na to još nisu odlučile, kao što su Slovačka, Turska, Portugal, Kina, Češka, Belgija, Austrija, Španija. Neke od pomenutih država, pre svih Španija i Portugal, čak prednjače u razvijanju novih pristupa i načina da se otkriju i kazne dela VTK. Činjenica da Konvencija nije formalno deo njihovog zakonodavstva nije sprečila razvoj unutrašnjih pravila, kao ni specijalizovanih organa – npr. Španija ima specijalne policijske jedinice i specijalne tužioce za VTK.

4) Najzad, pojedine države ne izražavaju značajan interes da razvijaju svoje zakonodavstvo u oblasti VTK. Ovakvih država je, na sreću, sve manje u svetu. Ipak, nikako ne može da raduje podatak da neke od država još uvek predstavljaju sigurno mesto za *cyber* kriminalce. Među ove retke izuzetke se mogu kvalifikovati Rusija, Maroko, Meksiko. Ovo ne znači da se u navedenim državama počinioci dela VTK ne gone. Oni se jednostavno svrstavaju u počinioce „običnih" krivičnih dela – npr. prevara izvedena na internetu se tretira kao krivično delo prevare; dečja pornografija je isto krivično delo bez obzira na sredstvo izvršenja, itd. Klasičan primer u tom pogledu je Meksiko. Rusija je, sa druge strane, slično „uredila" ovu oblast krivičnog prava. Ovakva rešenja nisu dobra, jer ne pretpostavljaju uvažavanje specifičnosti dela VTK. Iako smo svedoci da ruske policijske snage ulažu velike napore da se suzbije ekspanzija različitih oblika zloupotreba viso-

kih tehnologija, pojednostavljivanje cele jedne grupe kriminaliteta i njeno svođenje na svakodnevni kriminal može samo dovesti do apsurda kako u percepciji tih dela, tako i u procesuiranju njihovih počinilaca.

5. „*Cyber* pravosuđe“ u Srbiji

Kada se govori o savremenim tendencijama u pravu i pravosudnoj praksi, Srbija se obično može pomenuti kao neko ko nedovoljno brzo takve promene prati i ne prilagođava svoje zakonodavstvo novoj realnosti. Kod VTK ovo nije slučaj; državni organi su prepoznali potrebu da se ustroje specijalizovane institucije koje će se baviti istraživanjem, gonjenjem i sankcionisanjem dela koja su nastala korišćenjem visokih tehnologija, naročito računara i računarskih mreža. Iako je u mnogim aspektima Srbija na evropskom začelju kada je reč o *cyber* potencijalima – npr. procenat stanovništva koje svakodnevno koristi internet je među najnižima u Evropi, a prosečna brzina internet konekcije je desetostruko sporija od evropskog standarda – u Srbiji su rano počele da se identifikuju i žrtve i počinioci krivičnih dela putem računara. To je i bio razlog da se Srbija brzo uključi u evropske i svetske trendove suzbijanja ove vrste neželjenog ponašanja. Bez namere da se upustimo u detaljniju analizu srpskog zakonodavstva, navešćemo kratak pregled najvažnijih dešavanja koja su obeležila borbu protiv VTK u Srbiji:

• *Donošenje zakonskog okvira za delovanje*. Zakon o organizaciji i nadležnosti državnih organa za borbu protiv visokotehnološkog kriminala[22] i novi Krivični zakonik ustanovili su posebne organe, kao i posebna krivična dela VTK. Donošenje ovih zakonskih akata pokazalo je spremnost državnih institucija da se upuste u stvaranje dobrih preduslova da se Konvencija o visokotehnološkom kriminalu ratifikuje i da se VTK pridruži organizovanom kriminalu i ratnim zločinima kao poseban oblik kriminaliteta koji zbog svoje društvene opasnosti i složenosti delovanja zaslužuje specijalizovane timove za njegovo suzbijanje. U tom trenutku Srbija (u sklopu državne zajednice Srbija i Crna Gora) je bila jedna od mnogih zemalja koje su predstavljale pogodno tlo za *cyber* kriminalce – bez adekvatnog zakonodavstva, sa neiskusnom i needukovanim korisnicima računara i interneta. Čak ni zvanične institucije države, kao ni banke i drugi privredni subjekti nisu imali velikog iskustva u suprotstavljanju različitim oblicima zloupotreba visokih tehnologija.

---

[22] Službeni glasnik RS 61/05.

• *Implementacija donetih zakona* bila je druga faza na putu razvoja. Dugo se čekalo na realizaciju zacrtanog pomenutim zakonima. Najpre je počela da radi specijalna policijska jedinica, potom je (tek 2007. godine) izabran i prvi posebni tužilac, da bi najzad krenuli i procesi pred specijalnim odeljenjem Okružnog suda u Beogradu. U kratkom roku u kome funkcionišu, sve tri specijalizovane institucije pokazale su zavidan uspeh. Npr, u toku 2008. godine Posebnom tužilaštvu je podneto 166 prijava, koje su rezultirale podizanjem 75 optužnica, oduzimanjem 53 računara i 48400 diskova sa različitim autorskim delima koja su neovlašćeno distribuirana.[23]

• *Ratifikacija Konvencije o visokotehnološkom kriminalu Saveta Evrope i Dodatnog protokola uz konvenciju*. Ovo je svakako jedan od najvažnijih trenutaka u kratkoj istoriji borbe protiv VTK u Srbiji. Konvencija je, kao najdetaljniji i najprogresivniji dokument u ovoj oblasti, postala deo unutrašnjeg zakonodavstva Srbije. Obzirom da sudovi u Srbiji nemaju kulturu poštovanja ratifikovanih međunarodnih instrumenata, biće potrebno uneti odgovarajuće izmene u postojećem zakonodavstvu kako bi se ono usaglasilo sa Konvencijom. Ovo se pre svega odnosi na izmene važećih Krivičnog zakonika i Zakonika o krivičnom postupku, radi harmonizacije sa materijalnim i procesnim pravom Konvencije.

• *Izmene zakona*. Originalno, Posebno tužilaštvo je dobilo nadležnosti samo za dve grupe krivičnih dela, iz oblasti bezbednosti računarskih podataka i intelektualne svojine. Međutim, kao što se može videti i iz uporedne prakse, njegov domašaj mora da se prostire na sva dela koja su izvršena putem visokih tehnologija, a naročito na dečju pornografiju i dela prevare putem interneta, odnosno platnih kartica. Najvažnija izmena, osim onih koje su uslovljene celokupnom reformom sudskog i tužilačkog sistema u Srbiji, sadržana je u članu 2. Predloga Zakona o izmenama i dopunama Zakona o organizaciji i nadležnosti državnih organa za borbu protiv visokotehnološkog kriminala, kojim se član 3. važećeg Zakona menja tako da glasi:

„Ovaj zakon primenjuje se radi otkrivanja, krivičnog gonjenja i suđenja za:

1) krivična dela protiv bezbednosti računarskih podataka određena Krivičnim zakonikom;

2) krivična dela protiv intelektualne svojine, imovine, privrede i pravnog saobraćaja, kod kojih se kao objekat ili sredstvo izvršenja krivičnih dela javlja-

---

[23] Više podataka na zvaničnoj internet prezentaciji Posebnog tužilaštva za borbu protiv VTK: http://www.beograd.vtk.jt.rs/, 20.10.2009.

ju računari, računarski sistemi, računarske mreže i računarski podaci, kao i njihovi proizvodi u materijalnom ili elektronskom obliku, ako broj primeraka autorskih dela prelazi 2000 ili nastala materijalna šteta prelazi iznos od 1.000.000 dinara;

3) krivična dela protiv sloboda i prava čoveka i građanina, polne slobode, javnog reda i mira i ustavnog uređenja i bezbednosti Republike Srbije, koja se zbog načina izvršenja ili upotrebljenih sredstava mogu smatrati krivičnim delima visokotehnološkog kriminala, u skladu sa članom 2. stav 1. ovog zakona."[24]

Na osnovu rečenog kako o Srbiji tako i o drugim državama, može se zaključiti da je Srbija u prvoj grupi zemalja, koje su donele svoje zakonodavstvo, ratifikovale Evropsku konvenciju i uspešno je primenjuju. U tom smislu, Srbija se uspešno priključila narastajućem broju država koje se posebnim merama bore protiv VTK – njih je na početku XXI veka bilo svega petnaestak, a sada su države koje ignorišu ovaj problem retki izuzeci.[25]

Dragan Prlja, PhD
Mario Reljanović, LLM
Institute of Comparative Law, Belgrade

SYBERCRIME – COMPARATIVE EXPERIENCES

Cybercrime rapidly developed in last decade of 20th century, and in first years of 21st century its evolution is even more evident. States responded to this threat by introducing new measures into their legal systems, trying to reconcile traditional criminal law with new need to perce-

---

[24] U vreme pisanja ovog rada, Predlog zakona se nalazio u skupštinskoj proceduri za usvajanje. Ceo tekst Predloga zakona može se naći na internet prezentaciji Narodne skupštine Republike Srbije: http://www.parlament.gov.rs/content/lat/akta/akta_detalji.asp?Id=1033&t=P#, 20.10.2009.

[25] Bliže o razvoju specijalizovanog zakonodavstva država o VTK na internet adresi: http://www.cybercrimelaw.net/, 20.10.2009.

ive, investigate and prove newly introduced criminal offences. After the initial period of implementation of these measures, we can argue about their success, but also we have to point out defects of comprehensions that prevail in this field at the moment. Unification and harmonization, as well as efficient international cooperation, are basics for better coordination of transnational efforts to suppress cybercrime. Comparative analysis is not possible without review of the only relevant international document on cybercrime – Convention on Cybercrime of Council of Europe and pointing out its significance worldwide. Finally, we briefly deal with achievements of Serbia, as one of few countries that realized there is a need to introduce specialized state institutions to fight cybercrime and to set highest standards of implementation of all relevant legal and technical instruments in order to prevent misusage of high technologies.

Keywords: Cybercrime, Criminal Law, Privacy, Electronic Evidence; Comparative Study.