HRVATSKA AKADEMSKA I ISTRAŽIVAČKA MREŽA
CROATIAN ACADEMIC AND RESEARCH NETWORK

USPOREDNI PRIKAZ KAZNENOG ZAKONODAVSTVA REPUBLIKE HRVATSKE I STRANIH IZVORA U POGLEDU RAČUNALNOG KRIMINALITETA

CCERT-DOC-2006-03-1

CARNet CERT

Sigurnosni problemi u računalnim programima i operativnim sustavima područje je na kojem CARNet CERT kontinuirano radi. Rezultat tog rada ovaj je dokument za koji se nadamo se da će Vam koristiti u poboljšanju sigurnosti Vašeg sustava.

CARNet CERT, www.cert.hr - nacionalno središte za sigurnost računalnih mreža i sustava.

Autor: Tihomir Katulić, dipl.iur

SADRŽAJ

I. UVOD

Od nastanka prve verzije ovog dokumenta, nastale u studenom 2003., prošlo je više od dvije godine. Na području informacijske tehnologije dvije godine je puno vremena, no za ustroj zakonodavstva dvije godine obično ne znači mnogo. Ipak, informacijska tehnologija i promjene koje ona donosi sve više ubrzavaju i procese koji se nekad trajali desetljećima.

Efikasnost zakona kao upravljačkog mehanizma društva velikim dijelom ovisi o dva faktora. Jedan je svjesnost društva o (ne)ispravnosti određenog ponašanja, a drugi jest mogućnost institucionalizirane prisile u sprječavanju vrsta ponašanja koje društvo smatra pogubnim.

Drugim riječima, zakoni su tu da obavijeste članove neke zajednice o dozvoljenom i nedozvoljenom ponašanju, kao i da odrede kako nametnuti pravila koje društvo (ili tko već donosi zakone) smatra poželjnima. Podizanje svjesnosti društva o pravnim institutima sadržanim u zakonima trajan je proces, štoviše moglo bi se reći da je protek vremena upravo pretpostavka za ispunjenje ovog faktora.

Već smo rekli da dvije godine u pravnom i širem sociološkom smislu ne predstavljaju dug period. Zašto, onda, čitatelj pred sobom ima novu verziju dokumenta koji se u svojoj osnovi uglavnom bavi zakonodavnim rješenjima na području (zlo)upotreba informacijskih tehnologija?

Hrvatsko zakonodavstvo i pravni sustav u cjelini trajno brodi između dvije opasnosti, nedostatka odgovarajućih propisa s jedne strane, i normativnog optimizma s druge. Iako se ova izjava na prvi pogled može smatrati kontradiktornom, zapravo je jedina koja može opisati trenutak. Normativni optimizam, uvjerenje u rješavanje praktičnih problema u društvu kroz kontinuirano donošenje novih propisa, pojava je koja već godinama "krasi" naš pravni sustav. Neki pravni sustavi (primjerice, oni anglo-američke *common law* tradicije) nove zakone donose relativno rijetko. Koliko u Hrvatskoj osvane novih zakona čitatelj se može uvjeriti površnim pregledom Narodnih novina, službenog glasnika RH. Bez obzira tko je trenutno za kormilom, rješenje za svaku nedoumicu i problem svodi se na donošenje novog kamenčića u

zakonskom mozaiku. S druge strane, informacijska tehnologija napreduje mnogo brže i prodire mnogo dublje u svaku poru društva ostavljajući zakonodavca, a još više sudbenu vlast često u nedoumici. Hrvatska je u svoj pravni okvir u posljednje dvije godine uključila mnogo novih odredbi sadržanih u nekoliko zakonskih tekstova. U ovom novom pregledu pokušat ću predstaviti najvažnije odredbe, njihov *ratio* i posljedice.

Jedna od osnovnih ideja koja je potaknula nastanak prve verzije ovog dokumenta bila je vidjeti kako su pravni sustavi drugih zemalja riješili dilema koje Hrvatska upravo rješava. Izbor zemalja koje su uključene u Prikaz zasigurno će barem neki smatrati kontroverznim, no ovakav odabir uzima u obzir argumente kako pravne, tako i gospodarske i političke prirode.

Vjerujem da je prijašnja inačica ovog Prikaza bila koristan putokaz i zanimljivo štivo. S velikim zadovoljstvom primio sam vijest o uključivanju ovog dokumenta među izvore koji su poslužili za donošenje Nacionalne strategije informacijske sigurnosti, krovnog dokumenta donesenog od strane hrvatske Vlade, odnosno Središnjeg državnog ureda za e-Hrvatsku. Nadam se da će i ova nova verzija polučiti sličan uspjeh.

Tihomir Katulić

Zagreb, 10. studenog 2005.

II. PREGLED MATERIJALNOG ZAKONODAVSTVA RH

Nastavno na kratki komentar iznijet u uvodu ovog Prikaza, očito je da hrvatski pravni sustav pažljivo osluškuje promjene u pravnim porecima zemalja istovrsnog pravnog kruga. Većina pravnih stručnjaka slaže se da promjene u pravnom poretku trebaju biti evolutivne, a ne revolucionarne. Internet je u tehničkom smislu definitivno revolucija, ali u pravnom, a pogotovo u vezi s temom ovog rada, riječ je ipak o evolucijskoj promjeni.

U proteklih nekoliko godina hrvatski zakonodavac donio je nekoliko novih materijalnih propisa zbog sve većeg utjecaja modernih informacijskih tehnologija kako na gospodarstvo, tako i na život općenito. To su:

- **Zakon o zaštiti osobnih podataka NN 106/2003 (http://www.nn.hr/clanci/sluzbeno/2003/1364.htm)**
- **Zakon o elektroničkoj trgovini NN 173/2003 (http://www.nn.hr/clanci/sluzbeno/2003/2504.htm)**
- **Zakon o telekomunikacijama NN 122/2003 (http://www.nn.hr/clanci/sluzbeno/2003/1731.htm)**
- **Zakon o elektroničkom potpisu NN 10/2002 (http://www.nn.hr/clanci/sluzbeno/2002/0242.htm)**

Naravno, tu je i **Kazneni zakon** kao glavni oslonac kaznenopravnog sustava zakonodavstva RH, što je i logično mjesto da započnemo analizu hrvatskog zakonodavstva i njegovu trenutnu osposobljenost za bavljenje kažnjivim ponašanjima u digitalnoj eri.

1. Kazneni zakon RH

Kazneni zakon (NN 110/97) sa svojim izmjenama i dopunama, te *leges speciales*, ovisno o kojim povredama je riječ (**Zakon o autorskom pravu i srodnim pravima NN 167/2003)**, već navedeni novi propisi vezani uz upotrebu informacijske tehnologije čine sustav hrvatskog kaznenog zakonodavstva. Slijedeći ustavno načelo o određenosti kaznenih djela, bitno svojstvo kaznenog prava jest da je postojanje zakonske definicije kažnjivog ponašanja kao kaznenog djela nužan preduvjet

kaznenog progona. Drugim riječima, bez zakonske odredbe kojom se neko ponašanja kvalificira kao kazneno djelo, nema mogućnosti primjene kazne i drugih mjera na počinitelja. Kazneni zakon je osnovni propis koji sadrži definicije velikog broja kaznenih djela iz svih područja života, pa tako i s područja *cybercrime-a*, no kaznena djela opisana su i u drugim zakonima. Uobičajeno je da se kaznena djela specifična za određenu aktivnost nalaze u specijalnom zakonu koji regulira dotično područje. Tako je i kod nas, kao što će biti vidljivo iz priloženog.

Od vremena nastanka prošlog Prikaza, **Kazneni zakon** doživio je nekoliko promjena. Odredbe koje smo 2003. opisali i koje su trebale biti dio kaznenog zakonodavstva zapravo nisu zaživjele[1]. Razlog tome je političke prirode, vezan za neke druge kaznene odredbe koje su također bile dio novele, i za koje kod zakonodavca nije postojao potreban konsenzus.

Početkom srpnja 2003. ipak je donesena novela **Kaznenog zakona** koja se primjenjuje od 1.listopada 2004. Ovom novelom, objavljenom u službenom glasniku RH (Narodne Novine br. 105/2004) čl. 223 je doživio veliku izmjenu, i sad se zove **Povreda tajnosti, cjelovitosti i dostupnosti računalnih podataka, programa ili sustava** i obuhvaća sve odredbe poglavlja Konvencije o kibernetičkom kriminalitetu o tajnosti, nepovredivosti i dostupnosti podataka spremljenih na računalima i samih računala. Za ova kaznena djela biti će kažnjiv i pokušaj [2].

---

[1] Stari čl. 223, Oštećenje i upotreba tuđih podataka, pokrivao je samo kaznena djela Neovlaštenog pristupa i Oštećenja, izmjene i uništenja podataka (čl. 2 i 4. Konvencije).

[2] Čl. 223 **Povreda tajnosti, cjelovitosti i dostupnosti računalnih podataka, programa ili sustava** sada glasi:
(1) Tko unatoč zaštitnim mjerama neovlašteno pristupi računalnim podacima ili programima, kaznit će se novčanom kaznom ili kaznom zatvora do tri godine.
(2) Tko onemogući ili oteža rad ili korištenje računalnih sustava, računalnih podataka ili programa ili računalnu komunikaciju,kaznit će se novčanom kaznom ili kaznom zatvora do tri godine.
(3) Tko ošteti, izmijeni, izbriše, uništi ili na drugi način učini neuporabljivim ili nedostupnim tuđe računalne podatke ili računalne programe,kaznit će se novčanom kaznom ili kaznom zatvora do tri godine.
(4) Tko presreće ili snimi nejavni prijenos računalnih podatka koji mu nisu namijenjeni prema, unutar ili iz računalnog sustava, uključujući i elektromagnetske emisije računalnog sustava koji prenosi te podatke, ili tko omogući nepozvanoj osobi da se upozna s takvim podacima,kaznit će se novčanom kaznom ili kaznom zatvora do tri godine.
(5) Ako je kazneno djelo iz stavka 1., 2., 3. ili 4. ovoga članka počinjeno u odnosu na računalni sustav, podatak ili program tijela državne vlasti, javne ustanove ili trgovačkog društva od posebnoga javnog interesa, ili je prouzročena znatna šteta, počinitelj će se kazniti kaznom zatvora od tri mjeseca do pet godina.

Osim toga, dodani su članci 223.a **Računalno krivotvorenje** i 224.a **Računalna prijevara**. Uveden je i članak 197a, **Dječja pornografija na računalnom sustavu ili mreži**[3]**.** Što se tiče čl. 3 Konvencije o kibernetičkom kriminalitetu i tamo opisanog djela neovlaštenog presretanja podataka (Illegal Interception) kojeg prethodna varijanta čl. 223. nije pokrivala, novi članak 223. sada sadrži odredbe o neovlaštenom presretanju podataka i o kompjutorskoj špijunaži.

2. Zakon o telekomunikacijama

Zakon o telekomunikacijama iz 2003. posebnu je pažnju javnosti privukao svojim odredbama iz članka 111. kojima je prvi put u hrvatski pravni sustav uveden pojam *spam-a*, odnosno neželjenih reklamnih poruka. Primijenjeno je rješenje već poznato iz poredbenog prava. Sličan sustav primijenilo je i federalno zakonodavstvo SAD u Digital Millenium Actu, naglašavajući da je *spam* svaki *unsolicited commercial e-mail*, odnosno, da je riječ o reklamnoj poruci koja je poslana bez prethodnog odobrenja potrošača.

Predviđena su dva seta novčanih kazni različite visine, ovisno da li je prijestupnik pravna ili fizička osoba, i to u iznosima od 1,000-10,000 kn za fizičke i 5,000-1,000,000 kn za pravne osobe. Dok je okvir za pravne osobe adekvatan, visina odgovornosti za fizičke osobe preniska je uzme li se u obzir potencijalna korist koju štetnik od ovog vida zloupotrebe IT resursa može imati. U hrvatskom pravosuđu još

---

(6) Tko neovlašteno izrađuje, nabavlja, prodaje, posjeduje ili čini drugome dostupne posebne naprave, sredstva, računalne programe ili računalne podatke stvorene ili prilagođene za činjenje kaznenog djela iz stavka 1., 2., 3. ili 4. ovoga članka, kaznit će se novčanom kaznom ili kaznom zatvora do tri godine.
(7) Posebne naprave, sredstva, računalni programi ili podaci stvoreni, korišteni ili prilagođeni za činjenje kaznenih djela, a kojima je počinjeno kazneno djelo iz stavka 1., 2., 3. ili 4. ovoga članka oduzet će se.
(8) Za pokušaj kaznenog djela iz stavka 1., 2., 3. ili 4. ovoga članka počinitelj će se kazniti.

[3] Članak 197.a KZ-a, «Dječja pornografija na računalnom sustavu ili mreži» sada glasi:
(1) Tko pomoću računalnog sustava ili mreže proizvodi, nudi, distribuira, pribavlja za sebe ili drugoga, ili tko u računalnom sustavu ili na medijima za pohranu računalnih podataka posjeduje pornografske sadržaje koji prikazuju djecu ili maloljetnike u seksualnom eksplicitnom ponašanju ili koji su fokusirani na njihove spolne organe, kaznit će se kaznom zatvora od jedne do deset godina.
(2) Tko djetetu, posredstvom računalnog sustava, mreže ili medija za pohranu računalnih podataka učini pristupačnim slike, audiovizualne sadržaje ili druge predmete pornografskog sadržaja, kaznit će se novčanom kaznom ili kaznom zatvora do tri godine.
(3) Posebne naprave, sredstva, računalni programi ili podaci korišteni ili prilagođeni za počinjenje kaznenog djela iz stavka 1. i 2. ovoga članka oduzet će se

nije zabilježen slučaj kažnjavanja po ovim zakonskim osnovama. Veliko je pitanje, uzme li se u obzir sudska praksa za slična kaznena djela, da li će biti iskorištene zakonske odredbe u potpunosti.

Također, prema odredbama Zakona o izmjenama i dopunama zakona o telekomunikacijama (NN 70/05) i Pravilnika o osnovnim telekomunikacijskim uslugama (NN123/05) određeno je pravo na prigovor korisnika telekomunikacijskih usluga u slučajevima kada je prouzročena šteta uslijed zaraze računala malicioznim programima – *dialerima.*

Nadgledanje ovog i drugih prekršaja te kaznenih djela navedenih u Zakonu o telekomunikacijama spada prvenstveno u nadležnost Ministarstva, Agencije za telekomunikacije i Državnog inspektorata.

3. Zakon o elektroničkoj trgovini

U prvom članku Zakona o elektroničkoj trgovini definirano je njegovo polje primjene koje se sastoji u uređenju pružanja usluga informacijskog društva, odgovornosti davatelja usluga informacijskog društva, te pravilima u vezi sa sklapanjem ugovora u elektroničkom obliku. Posebno je važan članak 9. čijim odredbama je i u hrvatskom zakonodavstvu elektronička trgovina priznata kao legitiman oblik trgovine, ni po čemu manje vrijedna od ostalih (čl.9 st.3). Ipak, primjetan je strah zakonodavca od mogućih zloporaba elektroničke tehnologije kroz široko formuliranu limitirajuću klauzulu u stavku 4. istog članka.

Zakon je odredio obveze pružatelja Internet usluga i njihovih korisnika, pogotovo u pogledu privremene pohrane podataka (cachinga), pohrane podataka (web-hostinga) i odgovornosti pružatelja Internet usluga u skladu s obvezama preuzetima u okviru Konvencije o kibernetičkom kriminalitetu. Tako je, primjerice, za pružatelja Internet usluga predviđena obveza pohrane podataka kako bi isti mogli biti korišteni u eventualnim kaznenim ili prekršajnim postupcima zbog djela počinjenih putem Interneta.

Nadalje, u članku 23 Zakona o elektroničkoj trgovini uvedene su odredbe o prekršajnom kažnjavanju pravne osobe – pružatelja usluga informacijskog društva[4].

4. Zakon o elektroničkom potpisu

Pitanje da li je jedna od ugovornih strana zaista onaj koji se predstavlja da jest, odnosno da li posjeduje ovlasti da bi o nečemu pregovarao, jest jedno od onih pitanja vezanih uz ljudsku prirodu koje daleko po starosti nadmašuje svaku tehnologiju, pa tako i ovu vezanu uz računala i Internet.

Prilikom sklapanja ugovora putem e-maila, najsigurniji način zaštite zasad je onaj putem elektroničkog potpisa. I hrvatski zakonodavac prihvatio je upotrebu tehnologije digitalnog potpisa **Zakonom o elektroničkom potpisu** objavljenom u Narodnim novinama br. 10 od 17. siječnja 2002.

Što je konkretno elektronički potpis? To je *skup mjera koje osiguravaju pouzdanu identifikaciju korisnika elektroničkih komunikacijskih tehnologija, odnosno, zakonskom terminologijom*[5] :

"Napredni elektronički potpis" je, elektronički potpis koji je povezan isključivo s potpisnikom, nedvojbeno identificira potpisnika, nastaje korištenjem sredstava kojima potpisnik može samostalno upravljati i koja su isključivo pod nadzorom potpisnika, te sadržava izravnu povezanost s podacima na koje se odnosi i to na način koji nedvojbeno omogućava uvid u bilo koju izmjenu izvornih podataka".

Što to zapravo znači? Prvenstveno, riječ je o skupu mehanizama, softverskih tehnologija, koje će nedvojbeno moći povezati neku e-mail poruku sa određenim, zaista postojećim fizičkim ili pravnim subjektom.

Drugo, riječ je o zakonskoj najavi primjene tehnologije koja se kolokvijalno naziva **PKI**, odnosno Public Key Infrastructure[6]. To je metoda koja ujedinjuje korisnika koji treba biti potvrđen, i specijalnu tvrtku ili ustanovu koja jamči točnost

[4] Ovo je nova kategorija uvedena čl.2 predmetnog Zakona koji kaže da je …" Usluga informacijskog društva – usluga koja se uz naknadu pruža elektroničkim putem na individualni zahtjev korisnika, a posebno Internet prodaja robe i usluga, nuđenje podataka na Internetu, reklamiranje putem Interneta, elektronički pretraživači, te mogućnost traženja podataka i usluga koje se prenose elektroničkom mrežom, posreduju u pristupu mreži ili pohranjuju podatke korisnika"

[5] Čl. 4. Zakona o elektroničkom potpisu

[6] Henry H. Perritt, Jr., *CyberPayment Infrastructure*, 1996 JOURNAL of the ONLINE LAW. art. 6

podataka, u zajedničkom naporu da osiguraju jedinstveni, težak za krivotvorenje, identitet korisnika – ugovorne stranke na Internetu.

U vezi s navedenim, doneseni su i specijalni propisi koji taksativno nabrajaju dužnosti pravnog subjekta koji će učestvovati u izradi elektronskog potpisa. Ti propisi su:

a) **Pravilnik o registru davatelja usluga certificiranja elektroničkih potpisa koji izdaju kvalificirane certifikate** (Narodne Novine 54/02)
b) **Pravilnik o mjerama i postupcima uporabe i zaštite elektroničkog potpisa i naprednog elektroničkog potpisa, sredstava za izradu elektroničkog potpisa, naprednog elektroničkog potpisa i sustava certificiranja i obveznog osiguranja davatelja usluga izdavanja kvalificiranih certifikata** (Narodne Novine 54/02)

Naravno, niti hrvatski zakonodavac nije sasvim imun na negativni publicitet koji okružuje trgovinu na Internetu. Zato je u navedenom zakonu o elektroničkom potpisu uveo i niz odredbi koje ozbiljno osakaćuju mogućnost da se ozbiljniji ugovori sklapaju putem Interneta. S rezervama[7] uključenim u članak 6. Zakona o elektroničkom potpisu ozbiljno je smanjen broj ugovora koje je moguće sklopiti na ovaj način, pogotovo zato što su odredbe 8. i 9. stavka 2 čl. 6. često u sastavu mnogih zakona i drugih propisa koji reguliraju različite vrste ugovornih odnosa.

Problemom vjerodostojne autentifikacije pozabavio se i **UNCITRAL**[8] u svom model zakonu o elektroničkoj trgovini, konkretno u članku 7. Zanimljiv je komentar (glava 52. komentara ovog model zakona) o praksi mnogih država koja kod sklapanja

[7] Članak 6. Zakona o elektroničkom potpisu glasi:

"Ne može se odbiti prihvaćanje dokumenta samo zbog toga što je sačinjen i izdan u elektroničkom obliku s elektroničkim potpisom ili naprednim elektroničkim potpisom.

Iznimno, stavak 1. ovoga članka ne odnosi se na:

1. pravne poslove kojima se vrši prijenos vlasništva na nekretninama ili se uspostavljaju druga stvarna prava na nekretninama,
2. oporučne poslove,
3. imovinske predbračne, odnosno bračne ugovore,
4. opterećenje i otuđenje imovine za koje je potrebno odobrenje centra za socijalnu skrb,
5. ugovore o predaji i raspolaganju s imovinom za života,
6. ugovore o doživotnom uzdržavanju i sporazume u svezi s nasljeđivanjem,
7. darovne ugovore "

određenih oblika ugovora - kupoprodaje zahtijeva potpis. Iz te je prakse vidljivo da mnogi pravni poreci smatraju prihvatljivim da umjesto vlastoručnog potpisa bude kao potpis specijalna perforacija papira, uređajem otisnut žig ili potpis da bi se ugovor smatrao valjanim. Mišljenje je **UNCITRAL**-ovih stručnjaka stoga da nema zapreka priznavanju adekvatno primijenjene tehnologije elektroničkog potpisa kao valjanog potpisa.

Članak 7. paragraf 1. pobliže određuje uvjete kad se smatra da je upotreba elektroničkog potpisa opravdana. Ti uvjeti uključuju:

- Ekvivalentan nivo sofisticiranosti opreme i komunikacijskih sustava u upotrebi između poslovnih partnera
- Prirodu i učestalost njihove trgovinske aktivnosti
- Vrstu i visinu transakcije
- Zakonski zahtjevi strankama u pogledu valjanosti potpisa
- Postojanje mehanizama osiguranja i naknade štete kod slučajeva neovlaštenog slanja poruka
- Poseban pogled prema praksi u relevantnoj industriji u vezi sa primjenom određene metode identifikacije itd.

O svemu ovdje navedenom, svoje je rekla i **ABA – American Bar Association**, odnosno američki savezni pandan našoj odvjetničkoj komori. To je mišljenje ukazalo potrebu definicije odgovornosti pružatelja usluga autorizacije korisnika, kao i za određenim, razumnim, stupnjem sigurnosti za potrošače i trgovce[9].

5. Ostali propisi koji sadrže kaznenopravne odredbe

U lipnju 2003. na snagu je stupio Zakon o zaštiti osobnih podataka. Članci 2-7 ovog zakona daju definiciju osobnih podataka i postupka obrade osobnih podataka[10]. Zakon

[8] UNCITRAL Model Law on Electronic Commerce with Guide to Enactment, 1996

[9] Information Security Committee, Electronic Commerce and Information Technology Division, Science and Technology Section, American Bar Association, DIGITAL SIGNATURE GUIDELINES: LEGAL INFRASTRUCTURE FOR CERTIFICATION AUTHORITIES AND ELECTRONIC COMMERCE (Draft October 5, 1995)

10 Čl. 2 st1 Zakona kaže: "…*Osobni podatak* je svaka informacija koja se odnosi na identificiranu fizičku osobu ili fizičku osobu koja se može identificirati"; Sam čin objavljivanja može se podvesti pod čl2.st2 Zakona, jer: "…*Obrada osobnih podataka* je svaka radnja ili skup radnji izvršenih na osobnim podacima, bilo automatskim sredstvima ili ne, kao što je prikupljanje, snimanje, organiziranje,

sadrži kaznene odredbe u čl. 36, kojim se određuje (novčana) kazna za izvršitelja obrade osobnih podataka koji prekorači granice svojih ovlasti ili osobne podatke prikuplja i obrađuje za drugu namjenu osim ugovorene. Također, izvršitelj obrade odgovara za davanje osobnih podataka na korištenje drugim korisnicima ili neprovođenje ugovorenih mjera zaštite osobnih podataka (članak 10. stavak 3.).

U trenutku nastajanja ove inačice Prikaza, naveliko se govori o još dva zakonska teksta koji su u različitim fazama zakonodavne procedure. Jedan od njih je Zakon o elektroničkom dokumentu, a drugi je Zakon o informacijskoj sigurnosti.

6. Hrvatsko materijalno zakonodavstvo i *cybercrime* – prolaz ili pad?

Materijalno zakonodavstvo samo po sebi prihvaća uvriježene svjetske standarde, ali ocjena sudske prakse i kaznenog postupanja, o čemu više u slijedećem poglavlju, nije toliko jednostavna. Svi do sada u praksi zamijećeni oblici zloupotrebe informacijske tehnologije opisani su u Kaznenom zakonu ili specijalnim zakonima poput Zakona o telekomunikacijama. Zakonski okvir za postupanje protiv počinitelja *cybercrimea* u Hrvatskoj postoji i spreman je za upotrebu.

Kako to, onda, da u medijima (a u sudskoj praksi pogotovo) ništa ili vrlo malo čujemo o kaznenom progonu počinitelja kaznenih djela kibernetičkog kriminaliteta? Problem leži u nedovoljnoj izobrazbi službenika policijskih uprava, državnog odvjetništva i konačno sudaca kaznenih odjela. Razlog ovome sigurno nije nedostatak stručnjaka koji bi mogli osposobiti navedene službenike. CARNet je nekoliko puta organizirao ili sudjelovao u organizaciji seminara o informacijskoj sigurnosti, no ono što je zaista potrebno jest inicijativa više razine izvršne vlasti koja će omogućiti da se takav prijenos znanja i informacija ustali, institucionalizira. Nedavno prihvaćeni Nacionalni program informacijske sigurnosti sadrži opsežan paket mjera[11] koje će, budu li provedene kako je zamišljeno, vrlo pozitivno utjecati na izgradnju informacijskog društva u Republici Hrvatskoj.

---

spremanje, prilagodba ili izmjena, povlačenje, uvid, korištenje, otkrivanje putem prijenosa, objavljivanje ili na drugi način učinjenih dostupnim, svrstavanje ili kombiniranje, blokiranje, brisanje ili uništavanje, te provedba logičkih, matematičkih i drugih operacija s tim podacima"

[11] Po novom Nacionalni programu informacijske sigurnosti nacionalni CERT središnje je nacionalno koordinacijsko tijelo za računalno-sigurnosne incidente u Republici Hrvatskoj

U svakom slučaju, institucije vezane uz kaznenopravni sustav na ovaj ili neki drugi način trebaju osposobiti svoje službenike i konačno početi aktivno provoditi propise, koji su bez svog ostvarenja u praksi i dalje poslovično mrtvo slovo na papiru.

III. CYBERCRIME I KAZNENI POSTUPAK U RH

Cilj ovog poglavlja Prikaza jest dati kratki pregled hrvatskog kaznenog postupka i pružiti osnovne informacije glede toka kaznenog postupka u svezi s pojavnim oblicima *cybercrime*-a. Mišljenje autora jest da širenje informacija i znanja o pokretanju i toku kaznenog i srodnih postupaka (u prvom redu prekršajnog) s ciljem progona pojavnih oblika *cybercrimea* može biti od pomoći i u prevenciji ovih kaznenih djela. Moderna filozofija kaznenog prava općenito manje stavlja naglasak na strogost kazne, a više na njenu neizbježnost, odnosno na neminovnost kažnjavanja društveno opasnih pojava u koje danas ubrajamo i *cybercrime.*

Već smo ranije spomenuli da Kazneni zakon iz 1998., sa svojim izmjenama i dopunama, te *leges speciales*, ovisno o kojim povredama je riječ (poput primjerice Zakona o autorskom pravu, Zakona o elektroničkoj trgovini, Zakona o telekomunikacijama ili Zakona o elektroničkom potpisu) čine sustav hrvatskog kaznenog zakonodavstva. Kada promatramo neko ponašanje za koje smatramo da šteti našim osobnim interesima i/ili ukupnom društvenom poretku, upravo je Kazneni zakon prvo mjesto gdje trebamo pogledati i vidjeti što o nekom djelu misli naš zakonodavac.

Međutim, materijalni zakoni, odnosno materijalno-pravne odredbe poput onih sadržanih u Kaznenom zakonu i drugim zakonima koji sadrže kaznene odredbe samo su pretpostavka za pokretanje kaznenog postupka. Kazneni postupak reguliran je posebnim postupovnim (procesnim) pravilima sadržanim u **Zakonu o kaznenom postupku.**

Ovaj dualizam propisa proizlazi iz nekoliko razloga, koji se uglavnom svode na očuvanje visoke razine pravne sigurnosti i efikasnosti. Kada bi i materijalne i procesne odredbe bile sadržane u istom propisu, svaka promjena takvog unificiranog krovnog propisa bila bi jak potres za cijeli sustav. Zato zemlje kontinentalnog pravnog sustava (poput Hrvatske) insistiraju na odvojenom uređenju materijalnih i procesnih odredbi. Vezano za problem kaznenog procesuiranja djela kompjutorskog kriminaliteta, odmah na početku valja istaknuti bitnu različitost kaznenog postupka od, primjerice, građanskog. Svrha odredaba kaznenog prava mogla bi se jednostavno

opisati kao skup propisa namijenjenih zaštiti društva od specificiranih neželjenih ponašanja. Neka od tih ponašanja (ubojstvo, krađa i u kontekstu kibernetičkog kriminaliteta, širenje dječje pornografije elektroničkim putem) posebno su opasna za društvo, pa ono nalaže njihovo procesuiranje **po službenoj dužnosti**. Drugim riječima, za pokretanje kaznenog postupka za neka kažnjiva ponašanja nije potreban službeni zahtjev oštećenog, već samo informacija kako bi pravosudna tijela mogla reagirati. Druga kaznena djela se procesuiraju tek na osnovu posebnih podnesaka, **privatne tužbe** ili **prijedloga za progon**.

Privatnu tužbu može podnijeti oštećenik za određeni, manji broj kaznenih djela u roku od tri mjeseca od kada je saznao za kazneno djelo i počinitelja. Ako oštećenik odustane od privatne tužbe, sud mora obustaviti postupak, a na glavnoj raspravi donijeti presudu kojom se optužba odbija. Tužba će se podnijeti općinskom sudu nadležnom za mjesto na kojem je djelo počinjeno ili pokušano, budući da je taj sud nadležan za procesuiranje kaznenih djela za koje je određena novčana kazna ili kazna zatvora do deset godina.

Za određena kaznena djela kazneni se postupak pokreće na prijedlog oštećene osobe ili druge ovlaštene osobe koji se podnosi državnom odvjetništvu u istom roku kao i privatna tužba sudu. Uloga državnog odvjetnika, njegovo pravo i obveza, jest progon kaznenih djela i zastupanje interesa društva i pojedinaca – oštećenika u kaznenim postupcima. Kada nastupa povodom kaznene prijave oštećenika državni odvjetnik je određen njegovom voljom i prijedlogom - kazneni postupak smije se pokrenuti samo kada nepobitno ustanovi postojanje prijedloga te mora od progona odustati ako oštećenik prijedlog povuče, a bez prijedloga oštećenika nije dopuštena nikakva radnja kaznenog progona.

1. Kazneni postupak u RH

Što hrvatski propisi govore o kaznenom postupku zbog počinjenja djela kibernetičkog kriminaliteta? Kazneni zakon RH ne specificira način pokretanja kaznenog postupka za ova djela, iz čega bi se moglo shvatiti da za kaznena djela iz čl. 223. Kaznenog zakona, kao i iz članaka 223a i 224a postupak pokreće državni odvjetnik po službenoj dužnosti. Međutim, Zakon o kaznenom postupku u članku 447. o skraćenom postupku navodi uvjete potrebne da bi se kazneni postupak odvijao prema odredbama o skraćenom postupku.

Skraćeni postupak relativno je novi institut kazneno-postupovnog prava osmišljen kako bi ubrzao procesuiranje kaznenih djela manje opasnosti za društveni poredak. Uvjeti o kojim članak 447. govori odnose se na visinu zaprijećene kazne koja ne može biti viša od 5 godina zatvora. Ovim uvjetima obuhvaćena su i kaznena djela iz čl 223 Kaznenog zakona, odnosno *cybercrime.* Znači, trenutno prevladavajuće mišljenje o pokretanju kaznenog postupka protiv kaznenih djela kompjutorskog kriminaliteta, a koje praksa još treba potvrditi ili osporiti, jest da se on provodi po odredbama skraćenog postupka.

U čl. 448 i 449. istog zakona navodi se da je temelj za pokretanje postupka **optužni prijedlog državnog odvjetnika** odnosno **privatna tužba oštećenika.**

Što čini optužni prijedlog u skraćenom postupku? Optužni prijedlog čine isti sastavni dijelovi kao i optužnicu, kako je i navedeno u čl 285 ZKP[12]. Iz tih sastavnih dijelova vidimo i koji su potrebni podaci kako bi se moglo imati uspjeha u kaznenom postupku.

[12] 1) ime i prezime okrivljenika s osobnim podacima (članak 237.) kao i podacima o tome nalazi li se i otkad u pritvoru ili se nalazi na slobodi, a ako je prije podizanja optužnice pušten na slobodu, koliko je proveo u pritvoru,
2) opis djela iz kojeg proistječu zakonska obilježja kaznenog djela, vrijeme i mjesto počinjenja kaznenog djela, predmet na kojemu je i sredstvo kojim je počinjeno kazneno djelo te ostale okolnosti potrebne da se kazneno djelo što točnije odredi,
3) zakonski naziv kaznenog djela, s navođenjem odredaba Kaznenog zakona koje se na prijedlog tužitelja imaju primijeniti,
4) naznaku suda pred kojim će se održati glavna rasprava,
5) prijedlog o dokazima koje treba izvesti na glavnoj raspravi, uz naznaku imena svjedoka i vještaka, spisa koje treba pročitati i predmeta koji služe za utvrđivanje činjenica,

Nakon zaprimanja optužnog prijedloga ili kaznene prijave oštećenika, državno odvjetništvo će **odlučiti o kaznenom djelu na temelju načela svrhovitosti.** Ovo konkretno znači da postoje neke zakonske mogućnosti i uvjeti na temelju kojih državno odvjetništvo može odustati od kaznenog progona. O tim mogućnostima i uvjetima govori nam čl. 184 ZKPa. Ipak, da bi došlo do primjene njegovih odredaba potreban je i pristanak oštećenika, koji ga naravno nije dužan dati, odnosno koji može odlučiti nastaviti s kaznenim progonom[13].

Zakon o kaznenom postupku jedan je od nomotehnički složenijih domaćih propisa, pa su različita mišljenja o njegovim odredbama česta i među kaznenopravnim profesionalcima.

2. Sudska praksa

U pogledu procesuiranja kaznenih djela kompjutorskog kriminaliteta, radi višeg stupnja pravne sigurnosti potreban nam je čvrst oslonac na praksu, koje nažalost zasad (osim u pogledu klasičnih kaznenih djela počinjenih putem novih tehničkih sredstava poput Računalnog krivotvorenja, Računalne prijevare i Dječje pornografije na računalnom sustavu ili mreži) nema dovoljno. Koliko je autoru poznatu u trenutku nastanka ovog Prikaza hrvatsko pravosuđe nije kazneno obradilo niti jedan slučaj koji bi upućivao na neko od kaznenih djela specificiranih čl. 223 (Povreda tajnosti, cjelovitosti i dostupnosti računalnih podataka, programa ili sustava) Kaznenog zakona RH.

[13] Članak 184.
(1) Osim kad mu je to po zakonu dopušteno, državni odvjetnik može odlučiti da odgodi početak započinjanja kaznenog progona ako je kaznena prijava podnesena za kazneno djelo za koje je predviđena novčana kazna ili kazna zatvora do tri godine, a djelo je nižeg stupnja krivnje kod kojega razmjeri štetnih posljedica ne nalažu javni probitak kaznenog progona. Rješenje o odgodi početka kaznenog progona državni odvjetnik može donijeti samo uz prethodnu suglasnost oštećenika i privolu osumnjičenika i njegovu pripravnost da ispuni jednu ili više od sljedećih obveza:
1) izvršenje kakve činidbe u svrhu popravljanja ili naknade štete prouzročene kaznenim djelom,
2) uplata određene svote u korist javne ustanove, u humanitarne ili karitativne svrhe, odnosno u fond za naknadu štete žrtvama kaznenih djela,
3) ispunjenje obveze zakonskoga uzdržavanja,
4) obavljanje rada za opće dobro na slobodi

Na polju zaštite autorskog prava hrvatska policija postigla je određene uspjehe u suradnji s udruženjima koja štite autorsko i srodna prava, poput BSA[14] ili ZAMP[15]. Kako bi se pomoglo naporima policije u hvatanju počinitelja prekršaja i kaznenih djela, na stranicama BSA je moguće ispunjavanjem odgovarajućeg web-formulara anonimno prijaviti sumnjive slučajeve koje će BSA dalje proslijediti nadležnim organima. Iako postoji već solidan broj presuda za kaznena djela povrede autorskog i srodnih djela, kazne određene počiniteljima najčešće su uvjetne zatvorske ili novčane prirode uz oduzimanje predmeta kojima je kazneno djelo počinjeno.

Ako je cilj prevencija i kažnjavanje *cybercrimea,* u ovom trenutku jasno je da se težište u godinama koje dolaze preselilo sa zakonodavnog na strogo pravosudno. Iako se hrvatski pravni sustav ne oslanja primarno na sudske odluke kao precedentni izvor prava, sudska praksa koja sadrži stvarne presude bila bi snažna potpora i zalog pravne sigurnosti.

[14] BSA odnosno Business Software Alliance međunarodna je udruga proizvođača poslovnog softvera. BSA se bori protiv povrede autorskog prava svojih članica kroz razne inicijative koje za cilj imaju smanjenje stope piratstva i unapređenje kulture poštovanja intelektualnog vlasništva. Više o tome na www.bsa.org/hrvatska.

[15] **Hrvatsko društvo skladatelja – Zaštita autorskih muzičkih prava –** HDS ZAMP bavi se poslovima izdavanja odobrenja za sve vrste javnog korištenja glazbe na području Republike Hrvatske, ubiranjem autorskih naknada kao i raspodjelom već prikupljenih sredstava autorima u obliku autorskih honorara. Temeljem ugovora s Hrvatskom udrugom za zaštitu izvođačkih prava (HUZIP) i Hrvatskom diskografskom udrugom (HDU), HDS ZAMP i u ime spomenutih udruga prikuplja naknadu za prava izvođača i proizvođača zvučnih snimki. Više o ZAMPu na www.zamp.hr.

IV. VODIČ ZA PRIJAVU CYBERCRIME-a

Ovaj vodič namijenjen je svim pravnim i fizičkim osobama koje sumnjaju da je nad njima počinjeno neko od kaznenih ili prekršajnih djela o kojima je u ovom Prikazu riječ. Pokazati ćemo i ukratko skrenuti pažnju na određene postupke koji mogu maksimalno olakšati posao službama koje su nadležne za progon počinitelja.

Kao i kod progona svih kaznenih djela, autor apelira na potencijalne oštećenike da ne preuzimaju "stvari u svoje ruke". Uzvrat istim sredstvima (poput *Denial of service* napada ili slanjem *spama*) može samo naškoditi kako oštećeniku tako i svim ostalim pravnim i fizičkim osobama koje sudjeluju u procesu razmjene informacija elektroničkim putem, bilo kao pružatelji Internet usluga, poslovni partneri itd.

Već smo u poglavlju o kaznenom postupku kazali da se progon kaznenih djela kibernetičkog kriminaliteta razmatra u okviru odredaba o skraćenom postupku. Zakonodavac je time dao do znanja da smatra kako je riječ o kaznenim djelima manje važnosti pa je inicijativa o kaznenom progonu velikim dijelom (ali ne sasvim) na samom oštećeniku. Bez njegove privatne tužbe nadležnom općinskom sudu ili barem obavještavanja državnog odvjetnika kao državnog organa zaduženog za kazneni progon, kaznenog postupka protiv počinitelja neće biti. Kako se državni odvjetnik u pokretanju postupka rukovodi načelom svrhovitosti, državni odvjetnik može odlučiti da odgodi početak započinjanja kaznenog progona ako je kaznena prijava podnesena za kazneno djelo za koje je predviđena novčana kazna ili kazna zatvora do tri godine. Naravno, ovo vrijedi za djela nižeg stupnja krivnje kod kojih razmjeri štetnih posljedica ne nalažu javni probitak kaznenog progona i uz pristanak oštećenika, o čemu je već bilo riječi.

Upotreba Interneta povlači za sobom određene sigurnosne rizike. Bez upotrebe zaštitnih tehnologija poput *firewalla* ili antivirusnog softvera teško se može izbjeći zaraza i/ili kompromitacija računala. Problem kod otkrivanja pokušaja počinjenja kaznenih djela iz čl. 223 Kaznenog zakona RH leži u velikoj količini "napada" kojima je računalo u svakodnevnom radu na Internetu izloženo, a procjena o opasnosti koja od tih postupanja prijeti velikim dijelom također ovisi o stupnju iskustva korisnika

budući da tehničkih uvjeta za *"zero tolerance policy"* jednostavno nema. Ipak, konačnu procjenu o svrhovitosti kaznenog progona donijeti će državni odvjetnik, a ako oštećenik njome ne bude zadovoljan opcija privatne tužbe ostaje uvijek otvorena.

1. Potrebni podaci

Kako bi olakšali postupanje državnom odvjetniku i istražnim tijelima, preporuča se prikupljanje što je moguće više elektroničkih zapisa, *logova*, koji će istražnim tijelima poslužiti u otkrivanju počinitelja. Ovdje se u prvom redu misli na *firewall logove* i druge sistemske zapise koji sadrže podatke o aktivnostima na koje se oštećenik žali.

Prema odredbama Konvencije o kibernetičkom kriminalitetu pružatelji Internet usluga dužni su ustrojiti službe za obradu incidenata odnosno *cybercrimea.* Ovo je samo kodifikacija prakse koju već godinama provodi veliki broj najvećih svjetskih ISPova. Isto tako, i hrvatski *Internet provideri,* kako komercijalni tako i oni iz javnog sektora poput CARNeta, imaju organizirane slične službe, često kolokvijalno nazvane *Abuse* službama. Konvencija o kibernetičkom kriminalitetu predviđa i obvezu pružatelja Internet usluga da nadležnim organima učini dostupnima podatke o svom prometu. Iako se o tim odredbama Konvencije koje su od ISPova tražile tehničku sposobnost za pohranu podataka u određenom proteklom vremenskom periodu negativno očitovalo nekoliko svjetskih organizacija koje prate zaštitu osobnih podataka i privatnosti, postojeći sustav izjavljivanja *rezervi*[16] na primjenu Konvencije omogućio je njeno donošenje i stupanje na snagu[17].

Pružatelji Internet usluga u Hrvatskoj također su dužni pomoći nadležnim tijelima ukoliko to zahtijeva istražni postupak. Naravno, nadležna tijela, odnosno

[16] Rezerve na tekst neke konvencije omogućuju da tekst bude prihvatljiviji većem broju država po cijenu neprihvaćanja nekih odredbi, najčešće onih za koje predlagatelj ne smatra da ih je ispočetka nužno prihvatiti. Ovaj mehanizam ugrađen je u mnoge svjetske multilateralne aktove, čime je znatno proširen njihov doseg.

[17] Konvencija o kibernetičkom kriminalitetu u čl. 42 i čl. 43 izrijekom navodi koje rezerve stranke Konvencije mogu izjaviti i pod kojim uvjetima. Tih rezervi je ukupno 9, a većinom se odnose na opise kaznenih djela ili dužnosti pravnih subjekata (npr. pružatelja Internet usluga). Tako, primjerice, čl.4 Konvencije koji govori o obvezi sankcioniranja kaznenih djela namjernog brisanja, oštećivanja ili mijenjanja podataka, omogućuje potpisnicama da ne primjene kriterij nanošenja ozbiljne štete kao sastavni dio bića tih kaznenih djela.

organi koji sudjeluju u istražnom postupku, dužni su ispuniti uvjete koje nalaže Zakon o kaznenom postupku kako bi dobili pristup podacima ISPa.

Kako prijaviti *cybercrime*?

Prvi korak svakog korisnika koji sumnja da je postao žrtvom nekog od oblika *cybercrimea* kontakt je s *Abuse*[18] službom svog pružatelja Internet usluga. Iako takve službe imaju ograničeno djelovanje, redovito zapošljavaju stručnjake koji će znati procijeniti ozbiljnost incidenta.

Iako, valja ponovno istaknuti, inicijativu za pokretanje kaznenog postupka imaju **isključivo** oštećenik i državni odvjetnik po prijedlogu ili informacijama dobivenim od strane oštećenika, to ne umanjuje ulogu ISPa odnosno njegove službe za obradu incidenata. Zbog tehničke prirode Interneta, mnogi incidenti ove vrste mogu vrlo lagano prerasti u postupke s međunarodnim elementom. Tada je iznimno važno imati uhodanu službu za obradu incidenata kako bi se u kontaktu s pružateljima Internet usluga u drugim zemljama moglo doći do potrebnih podataka koji bi otvorili mogućnost ustupanja kaznenog progona zakonodavstvu zemlje počinitelja.

Naravno, mišljenje *Abuse* službe o prirodi incidenta nije obvezujuće i oštećenik se u bilo kojem trenutku može obratiti direktno državnom odvjetniku ili policiji. Iz niza praktičnih razloga kaznena se djela i inače u pravilu prijavljuju policiji, budući da je policija dostupna u svakom trenutku, a njeni službenici su stalno na terenu i mogu najbrže reagirati na obavijest o počinjenom kaznenom djelu. Koliko je autoru poznato, hrvatska policija nema posebne organizacijske jedinice posvećene kibernetičkom kriminalitetu, već se tim područjem bave postojeće službe organizirane u okviru Ministarstva unutarnjih poslova.

Nakon zaprimanja prijedloga ili informacija o kaznenom djelu, državni odvjetnik će postupajući po Zakonu o kaznenom postupku podnijeti zahtjev istražnom sucu nadležnog općinskog suda – a to je sud na čijem je području kazneno djelo počinjeno ili pokušano. Daljnji istražni postupak ide po službenoj dužnosti i uglavnom neovisno o oštećeniku[19].

[18] Sigurnosni incidenti počinjeni od strane korisnika CARNet mreže prijavljuju se na adresu CARNetove Abuse službe abuse@carnet.hr

[19] Iako dotični može povlačenjem prijedloga zaustaviti daljnje postupanje

V. PREGLED ZAKONODAVSTAVA DRŽAVA

Uvid u kaznenopravne sustave država koji slijedi koristan nam je da steknemo predodžbu o načinima na koje različiti pravni sustavi rješavaju problem inkriminacije ponašanja koja čine djela kompjutorskog kriminaliteta. Zašto je to važno? Pravni poreci različitih država *različito* rješavaju iste situacije. Iako inicijative poput Konvencije o kibernetičkom kriminalitetu pokušavaju ujednačiti propise zemalja potpisnica, uspjeh gotovo nikad nije stopostotan.

Problemi nastaju kada pravni sustavi trebaju surađivati, što je kod kaznenog progona kibernetičkog kriminaliteta pravilo, a ne iznimka. Ilustrirajmo ovaj problem. U predizbornoj kampanji za predstavničko tijelo jedinice lokalne samouprave u RH, jedan od kandidata otkrio je kako je postao žrtvom klevete od strane protukandidata. Protukandidat je vodio *blog* koji to jasno dokazuje. Naš kandidat potražio je pravnu zaštitu kod odvjetnika, koji je nakon kratkog istraživanja otkrio da se *web* stranica u pitanju nalazi na području zemlje koja ima vrlo različit pravni sustav od RH, efektivno sprječavajući kazneni progon.

Upravo zato da bi se stekao kvalitetan uvid u mogućnost rješavanja ovog problema, izabrane su slijedeće države po ključu različitosti pravnog sustava, kao i relevantnosti za problem kompjutorskog kriminaliteteta općenito i u Hrvatskoj.

Kao i prije dvije godine biti će obrađeni pravni sustavi **Njemačke** i **Austrije**, kako zbog njihove gospodarske snage, tako i raširenosti (prodornosti) Interneta (a samim tim i mogućnosti proučavanja prakse kompjutorskog kriminaliteta) u tim zemljama. Naravno, to su i nama dva najbliža pravna poretka, izuzmemo li ostale zemlje nastale raspadom SFRJ koje također pripadaju istom pravnom krugu. U zemlje kontinentalnog pravnog kruga ubraja se i **Francuska**, za koju će se isto (ponovo) naći mjesta.

Pravni sustavi **Velike Britanije** i **SAD** svakako se trebaju naći u svakom komparativnom pregledu stranog prava. Riječ je o državama specifičnog, precedentnog (common law) sustava. Ti sustavi često sadrže vrlo osebujna i zanimljiva rješenja koja možda nisu često direktno upotrebljiva u zemljama kontinentalnog pravnog kruga. Ipak, kao što duga pravna tradicija i stabilni pravni

sustavi *common law* zemalja i pokazuju, ta su rješenja ponikla iz prakse i obično djeluju vrlo efikasno.

Posebno mjesto imaju **Kina** i **Japan**, koliko zbog svojih osebujnih pravnih sustava, toliko i zbog masivne Internet penetracije, te velikog broja sigurnosnih incidenata koji potječu iz tih zemalja. Iz ovog razloga, u ovogodišnju inačicu Prikaza uključen je i prikaz zakonodavstva **Brazila**, čiji su *hackeri* vrlo brzo stekli svjetsku reputaciju, što ne bi bilo moguće da i u toj zemlji nisu postojali potrebni uvjeti poput naglog uvođenja novih tehnologija i manjka zakonskih sankcija.

Iz očitih razloga, zanimljiva su nam i zakonodavstva nama neposredno susjednih zemalja, **Slovenije** i **Srbije i Crne Gore.** Na kraju, vidjeti ćemo i kako su kažnjiva ponašanja sankcionirana u **Švedskoj**, kao zemlji sa izrazito visokim stupnjem e-govermenta.

1. Kaznenopravno zakonodavstvo u Njemačkoj

Postoje dva glavna pristupa kaznenopravnom reguliranju kompjutorskog kriminaliteta. Jedan je izradom novih, specijalnih zakona, a drugi je dopunom postojećih. Oba ova pristupa imaju i dobre i loše strane, što možemo vidjeti i na njemačkom primjeru.

Među prvima u svijetu Nijemci su još 1970. u pokrajini Hessen donijeli zakon o zaštiti podataka. No, tek u **Saveznom zakonu o zaštiti podataka** iz 1977. unesene su kaznenopravne sankcije na području zaštite automatske obrade podataka.[20] Ipak, korpus modernog kaznenog prava u vezi s kompjutorskim kriminalitetom svodi se u Njemačkoj na slijedeće pravne izvore:

- **Drugi Zakon o sprječavanju gospodarskog kriminaliteta (Zweites Gesetz zur Bekampfung der Wirtschaftskriminalitat, 2.WiKG)**
- **Zakon o autorskom djelu**

Što su donijeli ovi zakoni? Njima su u korpus njemačkog Kaznenog prava uvedena slijedeća kaznena djela:

- krađa podataka (čl.202a WiKG)

[20] Doc.dr.sc. Dražen Dragičević, "Kompjutorski kriminalitet i računalni sustavi", str 171

- kompjutorska prijevara (čl.263a WiKG)
- kompjutorsko krivotvorenje (čl.269 WiKG)
- neovlašteno mijenjanje podataka (čl. 303a WiKG)
- ometanje rada računala ("Computersabotage", čl. 303b WiKG)
- zaštita autorskog prava na računalnim programima (čl.106 i 108 njemačkog Zakona o autorskom djelu)

Ipak, za razliku od mnogih zemalja, njemačko kazneno zakonodavstvo nije eksplicitno sankcioniralo kaznena djela samog neovlaštenog pristupa i neovlaštenog korištenja kompjutorskog sustava za osobne potrebe (tzv. krađa vremena[21]). Praksa njemačkih sudova u posljednje dvije godine otklanja dvojbe – neovlašteni pristup kazneno je djelo i u Njemačkoj.

Posebno, što se kaznenopravne zaštite koja se pruža piscima kompjutorskih programa tiče, ona je pružena kroz odredbe njemačkog zakona o zaštiti autorskog prava. Ta je zaštita sasvim u skladu sa direktivom EU iz 1991. o zaštiti kompjutorskih programa kroz autorskopravnu zaštitu (koja je provedena i kod nas, izjednačujući računalne programe s ostalim vrstama autorskih djela provedeno u **Zakonu o autorskom pravu**, kao i kaznenim djelom Povrede prava autora ili umjetnika izvođača, čl. 229 KZ te Neovlaštena upotreba autorskog djela ili izvedbe umjetnika izvođača, čl.230 KZ.

Usporedimo li njemačko zakonodavstvo sa smjernicama zadanim u Konvenciji o kibernetičkom kriminalu, vidimo da je njemačko zakonodavstvo u velikoj mjeri usuglašeno s relevantnom europskom legislativom. Nadalje, njemački sudovi imaju tridesetogodišnje iskustvo u rješavanju slučajeva vezanih za kompjutorski kriminalitet.

Za vrijeme pisanja prve verzije Prikaza postojale su neke dvojbe o sankcioniranju nekih oblika kibernetičkog kriminaliteta u njemačkom pravnom sustavu. Presuda njemačkog suda u slučaju autora crva "Sasser" Svena Jaschana otklonila je te sumnje – njemački pravni sustav efikasan je i osposobljen za provođenje standarda propisanih Konvencijom o kibernetičkom kriminalitetu. Nadalje, suradnja između njemačkog i drugih pravnih sustava (poput američkog)

[21] Doc.dr.sc. Dražen Dragičević, "Kompjutorski kriminalitet i računalni sustavi", str 176

vidljiva iz "Sasser" slučaja još je jedan dokaz da u Njemačkoj postoji interes i efikasan sustav kaznenog progona počinitelja *cybercrimea.*

2. Kaznenopravno zakonodavstvo u Austriji

Sve do 1987. austrijsko kazneno zakonodavstvo nije sadržavalo posebne odredbe u pogledu kompjutorskog kriminaliteta. Jedini propis u kojem su bile sadržane odredbe koje bi se ticale kompjutorskih zloporaba bio je **Zakon o zaštiti podataka** iz 1978.[22] Ipak, zaštita pružena ovim propisom odnosila se samo na osobne podatke građana pohranjene u javnim službama i ustanovama ovlaštenim za njihovo prikupljanje. Drugi kompjutorski podaci nisu uživali nikakvu zaštitu.

Na prijedlog austrijskog ministarstva pravosuđa 1985. predložena je nadopuna kaznenog zakonodavstva. Predlagano je da se u austrijski Kazneni zakon (**StrafGesetzbuch**, StGB) uvedu nova kaznena djela:

- oštećenje pohranjenih podataka
- kompjutorska prijevara
- kompjutorsko krivotvorenje
- krađa kompjutorskog vremena
- činjenje nedostupnim pohranjenih podataka

Iz navedenog se vidi da su austrijski i njemački stručnjaci surađivali, budući da su obje zemlje otprilike u isto vrijeme razmatrale reformu kaznenog sustava u pogledu obuhvaćanja kaznenih djela kompjutorskog kriminaliteta, na sličan način.

Prijedlog je djelomično prihvaćen, tako da su konačnu novelu **Strafgesetzbucha** unesena samo kaznena djela oštećenja podataka (čl. 126 StGB) i prijevarne zloupotrebe obrade podataka (čl. 148 StGB). Novi je Kazneni zakon stupio na snagu 1988. Za razliku od nekih drugih zemalja, koje su posebno inkriminirale kompjutorsku sabotažu, poput Njemačke, Japana, Brazila, Poljske i Kanade[23], Austrija se odlučila na slučajeve krađe ili oštećenja tehničke osnove (hardvera) primijeniti postojeće inkriminacije (čl. 127 Krađa, čl. 126 Teško oštećenje podataka) i uvesti novu inkriminaciju, oštećenje podataka (čl. 126a). Za počinjenu veću štetu

[22] Doc.dr.sc. Dražen Dragičević, "Kompjutorski kriminalitet i računalni sustavi", str. 167.
[23] Doc.dr.sc. Dražen Dragičević, "Kompjutorski kriminalitet i računalni sustavi", str. 169.

zapriječena je i viša kazna (čl. 126a st.2.) Što se kaznenog djela prijevarne zloupotrebe obrade podataka iz čl. 148a tiče, biće ovog kaznenog djela obuhvaća kompjutorsku prijevaru i krivotvorenje putem programa, unosa, brisanja ili izmjene podataka, te svako drugo djelovanje kojim se utječe na tijek obrade podataka. Kao i u čl. 126. za ponavljanje kaznenog djela kao i za počinjenu veću štetu predviđena je i stroža kazna (kvalificirani oblik).

Novi austrijski propis o zaštiti privatnosti pomalo neočekivano (budući da i od Austrije potpisana Konvencija o kibernetičkom kriminalitetu predlaže kaznenu sankciju) odredio je prekršajno kažnjavanje neovlaštenog pristupa, transfer/emitiranje podataka te izbjegavanje ispravljanja netočnih podataka.

Iako je bilo za očekivati da će austrijski kazneni sustav teško odgovoriti na izazove kompjutorskog kriminaliteta ne sankcionira li preostala kaznena djela vezana uz kompjutorski kriminalitet, praksa austrijskih sudova govori drukčije. Uzimajući u obzir odredbe Konvencije o kibernetičkom kriminalitetu i usvojivši odgovarajuće smjernice EU poput "E-Commerce Directive" 2000/31/EC, austrijski pravni sustav redovito sankcionira pojavne oblike *cybercrimea*, u čemu mu pomažu i agencije poput STOPLINEa[24]. Iako je STOPLINE prvenstveno usmjeren protiv dječje pornografije i neonacizma na Internetu, ova udruga surađuje s austrijskim pravnim sustavom i na drugim područjima *cybercrimea.*

3. Kaznenopravno zakonodavstvo u Velikoj Britaniji

Velika Britanija je sve do 1990. bila primjer zemlje koja je rješavala pitanja iz područja računalnog kriminala kroz postojeće propise. To su bili:

- **Theft Act (1968.)**
- **Forgery and Counterfeiting Act (1981.)**
- **Data Protection Act (1984.)**

Naravno, postojao je i propis o zaštiti autorskog i srodnih prava, tzv. **Copyright, Design and Patents Act (1988.)**

[24] STOPLINE je austrijska agencija organizirana od strane austrijskih pružatelja telekomunikacijskih usluga posvećena borbi prvenstveno protiv dječje pornografije i nacional-socijalističke propagande

1990. ipak donešen je i **Computer Misuse Act**, kojim su u kazneno zakonodavstvo uvedena konkretna kaznena djela kompjutorskog kriminaliteta.[25] Budući da je **Computer Misuse Ac**t jedan od starijih propisa te tematike, on u sebi sadrži samo tri inkriminacije, ali ako pozorno proučimo konkretne članke, biti će očito da je pokriven velik broj kompjutorskih delikata.

Koje su dakle inkriminacije navedene u ovom zakonu? Prva je tzv. temeljno (osnovno) kazneno djelo hacking-a (Basic Hacing Offence). U čl.2 definirano je Daljnje (kvalificirano) hakersko djelo (Ulterior Hacking Offence). Posljednje je u čl.3 Neovlašteno modificiranje kompjutorskog sadržaja. Budući da common law sustav nema sistematiku kontinentalnog pravnog kruga, objasniti ću navedene članke, na što se odnose, i koje sve slučajeve pokrivaju.

3.1 Osnovno djelo hackinga (basic hacking offence)

Prvi stavak čl.1 definira klasično kazneno djelo neovlaštenog pristupa. Elementi koji se traže u dispoziciji su volja (svijest) počinitelja da vrši kazneno djelo, neovlaštenost pristupa kao i sama činjenica da je pristup učinjen s računala na kojemu se nalaze podaci kojima nije dopušten pristup ili nekog drugog računala s njime povezanog.

Namjera počinitelja ne treba biti usmjerena na program ili podatke određene vrste ili program i podatke u nekom određenom kompjutoru.

U čemu se sastoji neovlašteni pristup? Britanski zakon široko definira neovlašteni pristup u 17. čl. navodeći da to podrazumijeva mijenjanje ili brisanje podataka, njihovo kopiranje ili premještanje, korištenje ili ispisivanje s kompjutora na kojem se nalaze na bilo koju lokaciju ili način[26].

3.2 Daljnje hackersko djelo (ulterior hacking offence)

Dok za kazneno djelo iz čl.1 zaprijećena kazna iznosi do 6 mjeseci zatvora ili odgovarajući novčani iznos, da je u čl.2 riječ o težem kaznenom djelu odmah je vidljivo po mogućnosti da bude primijenjena i kazna zatvora do pet godina. Ovaj je

[25] Doc.dr.sc. Dražen Dragičević, "Kompjutorski kriminalitet i računalni sustavi", str. 160
[26] Doc.dr.sc. Dražen Dragičević, "Kompjutorski kriminalitet i računalni sustavi", str. 162

članak, odnosno i samo kazneno djelo, zapravo nadgradnja na članak 1., jer da bi se čl.2 uopće mogao primijeniti potrebno da počinitelj izvršio kazneno djelo iz čl.1. Sam čl. 2. primjenjivanje sankcije uvjetuje počinjenjem kaznenog djela iz čl.1, namjerom da se izvrši ili olakša izvršenje nekog kaznenog djela za koje postoji zakonom točno utvrđena kazna (prijevara, krivotvorenje, iznuda itd.), a nebitno je hoće li se daljnje kazneno djelo izvršiti u isto vrijeme kad i djelo neovlaštenog pristupa ili nekom drugom prilikom[27]. Vrlo česti primjeri ovakvih djela su slučajevi hakera koji prilikom neovlaštenog pristupa kopiraju datoteke s brojevima kreditnih kartica. Pri tome uopće nije bitno da li je dalje kazneno djelo (prijevare, krivotvorenja) izvršeno.

3.3 Neovlašteno modificiranje kompjutorskog sadržaja

U čl.3. sadržano je kazneno djelo koje pokriva nekoliko kompjutorskih zloupotreba. Njime su obuhvaćene namjerne radnje počinitelja kojima je cilj:

- onemogućenje ili otežanje korištenja podataka
- onemogućenje ili otežanje korištenja programa
- onemogućenje ili otežanje korištenja samog računalnog sustava

Naravno, tumačenjem ovog članka može se obuhvatiti i sankcionirati djelovanje malicioznih programa, računalna prijevara i sabotaža. Prva osoba osuđena po ovom zakonu, u studenom 1995., bio je Christoper Pile, aka Black Baron, autor virusa Queeg i Pathogen, koji je svojim djelovanjem nanio štete u iznosu preko milijun funti.

Što je s usuglašenošću ovog zakona i Konvencije o kibernetičkom kriminalu? Iako inkriminacije nisu sistematizirane na isti način, sva potrebna kaznena djela već su dugo dio kaznenopravnog sustava, pa neke posebne izmjene na zakonodavnoj razini u proteklo vrijeme nisu ni bile potrebne.

Budući da je Ujedinjeno kraljevstvo država s *common law* pravnim sustavom, poput Sjedinjenih država i drugih država Commonwealtha, konkretni doseg ovog propisa ovisi o sudovima koji ga primjenjuju. Sudovi u common law sustavima imaju kreatornu ulogu, a njihove odluke (presedani) su bitan, stvarajući, izvor prava. Iako je

[27] Doc.dr.sc. Dražen Dragičević, "Kompjutorski kriminalitet i računalni sustavi", str. 163

riječ o državi bitno različite pravne tradicije od nas, zakonodavstvo i praksa britanskog pravosuđa ipak predstavljaju značajan izvor za usporedbu.

4. Kaznenopravno zakonodavstvo u SAD

Po svom unutarnjem ustrojstvu, SAD su federativna država. Jedna od posljedica takvog društvenog uređenja jest i svojevrsni dvostruki pravni poredak. Svaka od saveznih država ima svoj pravni poredak i set propisa, a za međudržavne (između saveznih država) i međunarodne sporove (SAD i neka druga država) načelno je zaduženo pravo federacije.

Što se kaznenog prava tiče, u federalnu domenu često spadaju i ponašanja za koja je zakonodavac smatrao da su previše bitna da bi bila prepuštena samo sustavima saveznih država. Takva su ponašanja sankcionirana na dva načina, uvrštavanjem u "**Federal Criminal Code**", znači opći federalni kazneni zakonik (dio općeg zakonika kaznenog i građanskog zakonika "**United States Code**") ili donošenjem novog zakona ("Act", poput npr. **Homeland Security Act** of 2002 ili **USA Patriot Act**).

SAD su potpisnik Konvencije o kibernetičkom kriminalu, i bilo je zanimljivo vidjeti kako su, barem na federalnoj razini, inkriminirana ponašanja označena kao kaznena djela u Konvenciji. SAD su svakako tehnološki predvodnik i zemlja sa najvišim stupnjem Internet penetracije, te su očekivano i izrazito pravno-tehnološki osviještena. Tako npr.

- u čl. 1030 federalnog kaznenog zakonika je sankcionirano kazneno djelo kompjutorskog krivotvorenja i prijevare,
- u čl. 1362 kazneno djelo ometanja normalnog funkcioniranja sustava (misli se na sustave pod državnom upravom)
- u čl. 2510 kazneno djelo neovlaštenog pribavljanja podataka (kompjutorske špijunaže),
- u čl. 2701 kazneno djelo neovlaštenog pristupa[28]

Naravno, SAD su i jedan od vodećih pravnih sustava po pitanju zaštite autorskog i srodnih prava. Propisi koji sadrže odredbe o autorskom i srodnim pravima

[28] http://www.usdoj.gov/criminal/cybercrime/fedcode.htm - popis federalnih propisa vezanih za kompjutorski kriminalitet.

vode računa i o mogućim povredama povezanim s korištenjem moderne informatičke tehnologije. Relevantni propisi s ovog područja su:

- **Copyright Felony Act**
- **Čl. 506, 2318 i 2319 US Code-a**
- **Digital Millenium Copyright Act (US Code čl. 1201-1205)**
- **The No Electronic Theft (NET) Act**[29]

Sasvim očekivano, pravni sustav SAD je otišao vjerojatno najdalje u zaštiti nesmetanog funkcioniranja kompjutorskih sustava i Interneta, što i ne čudi poznavajući gospodarsku važnost i snagu koju ta industrija ima u SAD. I sudska praksa i zakonodavstvo SAD do sada su bili značajan izvor podataka i iskustva kako za druge *common law* sustave tako i za ostale pravne sustave, a nema sumnje da će tu poziciju zadržati i u doglednoj budućnosti.

5. Kaznenopravno zakonodavstvo u Francuskoj

Kao i kod drugih zemalja kontinentalnog pravnog kruga, francusko je kazneno zakonodavstvo koncentrirano oko pisanog zakonika, donesenog od strane predstavničkog tijela (**Code Penale**).

Kaznena djela kompjutorskog kriminaliteta sadržana u francuskom Kaznenom zakonu su slijedeća[30]:

- neovlašteno pribavljanje podataka (kompjutorska špijunaža) čl.182
- kazneno djelo neovlaštenog pristupa (čl.323. st 1.)
- kazneno djelo mijenjanja sadržaja, brisanja ili oštećenja podataka (čl.323. st.2)
- kazneno djelo ometanja normalnog rada računala (čl. 323. st.2)
- kaznena djela prijevare i kompjutorskog krivotvorenja (čl. 323. st.3)

Iz navedenog se vidi da Francuska već godinama u potpunosti poštuje odredbe Konvencije o kibernetičkom kriminalu, budući da Code Penale sadrži sva kaznena

[29] http://www.usdoj.gov/criminal/cybercrime/iplaws.htm - lista propisa vezana za zaštitu autorskog i srodnih prava

djela koja je Konvencija o kibernetičkom kriminalu istaknula. Ovo ne iznenađuje previše, jer riječ je o zemlji koja ima snažnu zakonodavnu aktivnost, i koja je uvijek među prvima sankcionirala utjecaj novih tehnologija[31]. Pogotovo je to točno u građanskopravnoj sferi, gdje se, npr. kod problema odgovornosti tvrtki pružatelja Internet usluga često citira francuska zakonodavna i sudska praksa.

6. Kaznenopravno zakonodavstvo u Švedskoj

Kaznena djela kompjuterskog kriminaliteta su u švedskom kaznenopravnom sustavu sadržana u **Kaznenom zakonu**.

U poglavlju 4. Kaznenog zakona sadržana su u člancima 8, 9, 9a i 9c kaznena djela neovlaštenog pribavljanja podataka (kompjutorska špijunaža) (čl.8), neovlaštenog pristupa podacima ili kompjutorskom sustavu (čl. 9 i 9a) i kazneno djelo mijenjanja sadržaja, brisanja ili oštećenja podataka (9c).

Poglavlja 12. i 13. Kaznenog zakona sadrže klasične kaznenopravne odredbe o kaznenim djelima protiv imovine i kaznenopravnoj odogovornosti za štetu. Posebno se to odnosi na 13. poglavlje koje sadrži kaznena djela protiv države i dobrobiti građana. Ove se odredbe mogu primijeniti i na oštećenje i uništenje telefonske/radio i druge telekomunikacijske infrastrukture, pa tako i na počinitelje kaznenih djela onemogućenja pravilnog funkcioniranja kompjutorskih sustava[32].

Očigledno je da u Švedskoj postoji intencija zakonodavca da nova kaznena djela pokuša što je više moguće podvesti pod postojeće zakonske odredbe. Premda je takav pristup sasvim legitiman, i u načelu pridonosi načelu ekonomičnosti i efikasnosti funkcioniranja pravnog sustava u cjelini, postoje situacije kad je ipak bolje, bilo kroz reformu postojećeg propisa ili donošenje sasvim novog, jasno urediti neko područje. Dok njemačko, austrijsko i francusko iskustvo govori da i dopunjeni (novelirani) postojeći propis može služiti svrsi, mislim da bi u švedskom slučaju bilo bolje donijeti sasvim novi propis ili barem posebnu glavu vezanu uz kompjutorski

[30] Handbook of Legislative Procedures of Computer and Network Misuse in EU Countries for assisting Computer Security Incident Response Teams (CSIRTs), str. 47
[31] Vallerie Sedallian : " Controlling Illegal Content over the Internet", izlaganje održano u toku 26. International Bar Association Conference u Berlinu, 1996.
[32] Handbook of Legislative Procedures of Computer and Network Misuse in EU Countries for assisting Computer Security Incident Response Teams (CSIRTs), str. 72

kriminalitet u postojećem Kaznenom zakonu. Razlog tome je prilična neodređenost i široka formulacija dispozicija kaznenih djela u glavama 4, 12 i 13 koje, u trenutku nastajanja, nisu bile niti namijenjene pokrivanju područja kompjutorskog kriminaliteta. Ako švedski kaznenopravni propis ostane ovakav kakav jest, čak bez dodatnih novela koje bi malo "izoštrile sliku", uspješnost dosega propisa i pravna sigurnost ovisile bi isključivo o primjeni propisa od strane sudova, što u zemljama bez istaknute presedanske tradicije obično dovodi do izbjegavanja primjene sankcije na ponašanja koja nisu precizno obrađena u propisu koji treba primijeniti.

Razvoj događaja u posljednje vrijeme dao je za pravo prethodnoj ocjeni, budući da su nedavni pokušaji kažnjavanja korisnika peer-2-peer alata završili prilično neuspješno. U prvom takvom slučaju u ožujku 2005. javno tužiteljstvo je nakon dojave APB, švedske organizacije nositelja autorskih prava na glazbene i video sadržaje, pokrenulo postupak protiv počinitelja. APB je poslao preko 400,000 pisama upozorenja kršiteljima autorskog i srodnih prava kompanija čije interese zastupa, da bi se, zajedno s nekoliko ISP-ova, nedugo zatim suočio s preko milijun podnesaka koje su švedski građani podnijeli švedskim vlastima zbog povrede privatnosti. Naime, izuzetno strogi švedski standardi za zaštitu privatnosti odnose se i na privatnost na Internetu, pod što potpada i tajnost IP adrese, preko koje je APB došao do podataka o IP adresama. Kako je to jedini način da se ustanovi preko kojih računala se pomoću peer-2-peer alata šire zaštićeni sadržaji, ova se interesna udruga našla u vrlo nezgodnoj poziciji.

7. Kaznenopravno zakonodavstvo u Japanu

Pravni sustav Japana nakon Drugog svjetskog rata oblikovan je pod velikim utjecajem SAD. Za ovaj rad od značaja je krovni kaznenopravni propis, japanski Kazneni zakonik, kao i novi Zakon o neovlaštenom pristupu (**Unauthorized Computer Access Law** - Law No. 128 of 1999). Od prošlog Prikaza, na području japanskog kaznenog zakonodavstva dogodila se velika reforma Kaznenog zakonika, djelomično i pod utjecajem Konvencije o kibernetičkom kriminalitetu čija se ratifikacijska procedura u japanskom parlamentu, Dietu, približava kraju.

1. Inkriminacije iz dosadašnjeg Kaznenog zakonika:

- Kazneno djelo mijenjanja sadržaja, brisanja ili oštećenja podataka - Oštećenje privatnih podataka čl.259
- Kazneno djelo mijenjanja sadržaja, brisanja ili oštećenja podataka - Oštećenje javnih podataka čl.258

Budući da se novi Zakon o neovlaštenom pristupu bavi većinom preostalih kaznenih djela, čl. 258 i 259 su jedini relevantni glede kaznenih djela kojima je dispozicija vezana uz upotrebu računala (dalje slijede kaznena djela za čije ostvarenje načelno nije potreban kompjutor, ali japanski zakonodavac je problemu prišao na drukčiji način)

- Kazneno djelo krivotvorenja - čl.161.st2 JPC
- Kazneno djelo prijevare – čl. 246.st2. JPC[33]
- Kazneno djelo miješanja u poslovnu transakciju putem računala – čl 234.st.2

Ovdje je riječ o kaznenim djelima čije biće nije nužno vezano za korištenje računala. Mnoga zakonodavstva zato uz klasičnu dispoziciju ovih djela dodaju obično i stavak koji objašnjava modus počinjenja putem kompjutora. Japanski zakonodavac ipak je dodao uz postojeća kaznena djela krivotvorenja i prijevare posebna kaznena djela krivotvorenja i prijevare počinjena putem kompjutora. Ovo posebno vrijedi za Kazneno djelo miješanja u poslovnu transakciju putem računala – čl 234.st.2. Time je vjerojatno naglašena društvena zabrinutost zbog ugroženosti gospodarske grane od nacionalne važnosti. Ipak, uvođenjem ovakvih, paralelnih, kaznenih djela smanjuje se, a ne povećava pravna sigurnost, jer može doći do nedoumice oko ostvarenja ponašanja iz dispozicije kaznenog djela. Tradicionalan europski pristup, na određen način potvrđen u Konvenciji o kibernetičkom kriminalu ovdje ima prednost.

1. Inkriminacije iz Zakona o neovlaštenom pristupu (Unauthorized Computer Access Law - Law No. 128 of 1999)

- Kazneno djelo neovlaštenog pristupa (čl.3)
- Kazneno djelo omogućivanja neovlaštenog pristupa (čl.4)

[33] http://www.isc.meiji.ac.jp/~sumwel_h/Codes/comp-crim.htm

Ovaj zakon kroz navedene inkriminacije prilično precizno definira kažnjiva ponašanja, tako da obuhvaća u čl.3.st.2-1 klasično djelo neovlaštenog pristupa, zatim pod metodama na koji se način ono može počiniti uključuje i širenje i korištenje malicioznih programa. U članku koji slijedi kao kažnjivo ponašanje propisano je i odavanje informacija koje mogu omogućiti neovlašteni pristup.

Japansko zakonodavstvo u ovom trenutku još ne poznaje kazneno djelo ometanja normalnog rada računala (System Interference, čl. 5 Konvencije o kibernetičkom kriminalu), kazneno djelo neovlaštenog presretanja podataka (Illegal Interception, čl.3) niti tzv. "krađu vremena".

Što se tiče zaštite autorskog i srodnih prava, ovdje je očit američki utjecaj, budući da su relevantni propisi brojni i često ažurirani. Za ovaj Prikaz najbitniji je **Zakon o autorskom pravu** (Copyright Law), odnosno njegove kaznene odredbe sadržane u poglavlju 8, čl. 119. do 124. Ono što je ovdje posebno interesantno, uz standardni nivo zaštite koji se pruža svim autorskim i drugim zaštićenim djelima, jest čl. 120 a) koji predviđa novčanu kaznu u iznosu do milijun jena ili kaznu zatvora do 1 god. za svakog tko posjeduje, iznajmljuje ili prodaje uređaje čija je glavna svrha zaobilaženje tehničkih metoda zaštite autorskih i drugih zaštićenih djela.[34]

8. Kaznenopravno zakonodavstvo u Kini

Posljednjih je godina Kina usvojila nekoliko propisa i i upravnih mjera kojima je cilj zabraniti napade na kompjutorske sustave, nepravilna upotreba kompjutora i korištenje Interneta da bi se počinila kaznena djela. Glavni kaznenopravni propis, Kazneni zakonik (**Criminal Code**[35]) sam sadrži odredbe o kažnjavanju povreda vezanih uz kompjutorsku sigurnost. Od 1991. do sad uključene su i odredbe o kompjutorskim virusima, pružateljima Internet usluga, a kompjutorski softver je zaštićen kao i ostala prava intelektualnog vlasništva.

8.1 Propisi o zaštiti kompjutorskih sustava

Regulations on Safeguarding Computer Information Systems (1994.)

[34] Tekst Zakona o autorskom pravu : http://www.cric.or.jp/cric_e/clj/clj.html
[35] http://www.4law.co.il/316.pdf

Propis koji sadrži kaznena djela vezana uz kompjutorske sustave i kompjutorske mreže, koje sadrže kaznena djela poput neovlaštenog pristupa, ali i neka specifična kaznena djela isključivo vezana za kineski politički sustav, poput povrede obveze prijave i registracije međunarodno umreženih sustava (što bi značilo da sva međunarodno umrežena računala u Kini trebaju imati dozvolu da se umreže)

Sam Kazneni zakonik, kako sam već naveo sadrži neka klasična kaznena djela, poput:

čl.285 Kazneno djelo neovlaštenog pristupa zaštićenim računalima (ovdje su kao takva navedena računala koja sadrže informacije vezane za državne poslove, izgradnju vojnih instalacija ili znanstvenih ustanova, istraživanje i razvoj)

čl.286 propisuje kazne za počinjenje kaznenog djela brisanja, oštećenja ili mijenjanja podataka na zaštićenim kompjutorima kao i za onemogućenja pravilnog rada računala.

Kazneni zakonik sadrži i odredbe o kaznenim djelima počinjenim pomoću računala, poput prijevare, krađe, širenja dječje pornografije itd. Što se propisanih kazni tiče, premda su kaznena djela počinjena pomoću kompjutora posebno navedena, ipak se za određivanje visine kazne upućuje na temeljni oblik kaznenog djela, bez obzira na postojanje specifičnog oblika vezanog uz upotrebu računala. Ovakav pristup je elegantniji i bliži ostvarenju pravne sigurnosti, budući da postojanje paralelnih inkriminacija (npr. kaznenih djela prijevare, i prijevare počinjene putem računala) može unijeti nepotrebnu zbrku a time i pravnu nesigurnost.

Computer Information Network and Internet Security Protection and Management Regulations (1997.)

Tri godine poslije prvog propisa o mrežnoj sigurnosti uslijedio je novi propis, koji je dodao nova, kineskom sustavu svojstvena kaznena djela poput:

- iskrivljavanje istine i širenje glasina radi potkopavanja državnog poretka
- ugrožavanje reputacije državnih organa
- korištenje mreža i mrežnih resursa bez odgovarajuće dozvole

kao i kaznena djela čiju sankciju traži i Konvencija o kibernetičkom kriminalu, poput:

- stvaranje i širenje virusa

- onemogućivanje ispravnog rada kompjutora i kompjutorskih mreža te brisanje, oštećivanje i mijenjanje podataka

Measures for Administration of Prevention and Control of Computer Viruses (2000.)

Zanimljiv propis donesen u proljeće 2000. ustanovio je odgovornost državnih organa za poduzimanje mjera protiv širenja virusa, i mogućnost da zaposlenici u državnim organima budu kažnjeni za nepoduzimanje mjera koje unaprijeđuju računalnu sigurnost.

Kineski pravni sustav izrazito je specifičan, što je posljedica komunističkog režima. Premda se načelno smatra da se posljednjih godina Kina prilično reformirala i otvorila svijetu, iz ovog pregleda je očito da je kineski pravni sustav pod dominantnim utjecajem političkog sustava, o kojem ovisi i prihvaćanje odredaba Konvencije o kibernetičkom kriminalu. No, što se ovog pregleda tiče, ono što je relevantno je da i u Kini postoji organizirani napor i pristup sankcioniranju pojavnih oblika kompjutorskog kriminaliteta, i da sama Kina kao ogromno područje, sa sve većom Internet penetracijom posjeduje mehanizme kojima može kazniti počinitelje kaznenih djela vezanih za računala i Internet. Ipak, budući da mnogi od pojavnih oblika kompjutorskog kriminaliteta poput neovlaštenog pristupa i onemogućivanja ispravnog rada računala mogu biti iskorišteni i u neke druge svrhe, progon počinitelja ovisiti će isključivo o političkoj volji zbog prirode kineskog državnog uređenja.

9. Kaznenopravno zakonodavstvo u Brazilu

Površinom i brojem stanovnika najveća južnoamerička država u posljednje vrijeme može se pohvaliti i sve većim postotkom penetracije modernih telekomunikacijskih tehnologija. Budući da je općenita stopa kriminala u ovoj zemlji vrlo visoka, ne čudi mnogo da postoje i organizirane skupine koje se bave *cybercrime*-om. Upravo je brazilsko podzemlje[36] jedno od tehnološki najnaprednijih i najosviještenijih, ako je za vjerovati nedavno objavljenom izvještaju o stopi

[36] Među najpoznatije kriminalne grupe u Brazilu po izboru brazilskog H4ck3r: The Magazine of the Digital Underworld ubrajaju se Breaking Your Security, Virtual Hell i Rooting Your Admin. Brazilska policija godišnje zaprimi oko stotinu tisuća prijava kaznenih djela počinjenih putem Interneta, a jedini brazilski odjel policije koji se specijalizirao za *cybercrime*, lociran u glavnom gradu, sastoji se od desetak djelatnika

bankarskih i drugih elektroničkih prijevara koje Brazil svrstavaju na sam vrh tablice, a brazilskim hakerima pripisuju i mnoga djela izvan granica domovine.

Razlog ovakvom trendu, kao i uvijek, jest u spoju neodgovarajućeg pravnog okvira i nedovoljno opremljene i uvježbane policije i istražnih organa. Brazilski zakoni ne sadrže odredbe u skladu s Konvencijom o kibernetičkom kriminalitetu, a jedini zakon koji izrijekom barem djelomično pokriva neka od kaznenih djela specificiranih Konvencijom jest Zakon br. 9983 iz srpnja 2000., koji sadrži kaznena djela neovlaštene promjene i oštećenja podataka i informacijskog sustava. Iako brazilska praksa sadrži slučajeve kada su za kaznena djela počinjena putem Interneta određene i zatvorske kazne, riječ je uglavnom bila o kaznenim djelima prijevare počinjenim putem novog medija.

Iako se autor ne slaže s procjenom iznesenom za vrijeme Prve konferencije o *cybercrimeu* održane u Braziliji u ljeto 2004 koja navodi Brazil kao zemlju ishodište preko 80% sigurnosnih incidenata u 2003., činjenica je da ova zemlja uz Indiju i Kinu prednjači po broju počinjenih incidenata. Zabrinjavajuća je stopa porasta broja incidenata koja je od 20,000 u 2000. preko 50,000 u 2002 narasla na preko 100,000 krajem 2004.

10. Kazeno zakonodavstvo u Srbiji i Crnoj Gori

Od prošlog Prikaza zakonodavstvo Srbije i Crne Gore nije pretrpilo većih promjena na području kaznenog zakonodavstva, budući da je posljednjim izmjenama i dopunama **Krivičnog zakona Srbije**, izvršenim početkom 2003. (Službeni glasnik SRS 80/2002 i 39/2003) uvedeno nekoliko inkriminacija koje prije nisu postojale u srpskom kaznenom pravu, a koje odgovaraju djelima opisanima u Konvenciji o kibernetičkom kriminalu.

Računalnoj sigurnosti posvećena je čak jedna čitava glava u **Krivičnom zakonu**, glava 16a. (čl. 186a –186g). Tu su navedena slijedeća kaznena djela:

- Neovlašćeno korištenje računara i računarske mreže (čl. 186a)
- Računarska sabotaža (čl.186b)
- Pravljenje i unošenje računarskih virusa (čl.186c)
- Računarska prevara (čl.186d)

- Ometanje funkcionisanja elektronske obrade i prenosa podataka i računarske mreže (čl.186e)
- Neovlašćeni pristup zaštićenom računaru ili računarskoj mreži (čl.186f)
- Sprečavanje i ograničavanje pristupa javnoj računarskoj mreži (čl.186g)

Iz gore navedenog očito je da su naši istočni susjedi brzo i temeljito usvojili odredbe Konvencije o kibernetičkom kriminalu, tako što su u svoje kazneno pravo uveli sve inkriminacije iz Konvencije o kibernetičkom kriminalu[37].

Što je s kaznenopravnom zaštitom autorskih prava kod naših istočnih susjeda? Naslijeđujući propise bivše zajedničke države, i zaštita autorskog i drugih srodnih prava već je odavno našla mjesto i u njihovom kaznenom zakonodavstvu. Tome svjedoči i čl 183a. Neovlašteno korištenje autorskog i drugog srodnog prava.

11. Kaznenopravno zakonodavstvo u Sloveniji

Kakva je situacija kod naših zapadnih susjeda? Pojavni oblici kompjutorskog kriminaliteta u zakonodavstvu Slovenije su koncentrirani u slovenskom kaznenom zakoniku ("**Kazenski zakonik**"). Prvim reformama iz 1995., kada je donesen i novi **Zakon o autorskom pravu**, počeo je proces usvajanja kaznenopravnih standarda u kažnjavanju pojavnih oblika kompjutorskog kriminaliteta.

1999. novom je reformom kaznenog sustava u slovenski kazneni zakon uneseno i kazneno djelo neovlaštenog pristupa kompjutorskom sustavu kao i kazneno djelo neovlaštenog mijenjanja sadržaja, uništenja ili oštećenja podataka[38].

Iste je godine noveliran i Zakon o autorskom pravu, a time i kazneni zakon u koji su sad uključena i kaznena djela vezana uz povredu autorskog i srodnih prava[39]. Nakon ove novele u kaznenopravni sustav uključena su bila i kaznena djela vezana uz neovlašteno korištenje autorskih djela, kršenje autorskog i drugih srodnih prava (čl. 158., 159. i 160. Kazenskog zakonika). Novom promjenom Zakona o autorskom pravu iz 2004. Slovenija je uvela još strožije mjere koje bi trebale utjecati na daljnje smanjenje stope piratstva.

[37] http://www.projuris.org/aktuelno_comp_kriminal.htm
[38] Register predpisov Slovenije, Ur.l. RS, št. 23/99, čl.225
[39] http://www.aas.si/pravni-viri/kzrs-fr1.html

Prema nekim podacima, objavljenima i u glasilu udruge Business Software Alliance (BSA) i srpskog časopisa Ekonomist[40] Slovenija je, kao i većina ostalih bivših komunističkih zemalja početkom devedesetih imala visoku stopu piratstva, negdje oko 90%. Očigledno da su donešeni propisi postigli svoju svrhu, budući da prema izvješću BSA za 2005. Slovenija ima manje od 60% nelegalnog softvera, štoviše velik dio tog broja otpada na takozvano "meko piratstvo", odnosno na korištenje službenih licenci na većem broju računala od dopuštenog.

U ovom trenutku, Slovenija ispunjava sve zahtjeve Konvencije o kibernetičkom kriminalu.

[40] http://www.ekonomist.co.yu/magazin/ebit/12/por/slovenc.htm

VI. KONVENCIJA O KIBERNETIČKOM KRIMINALITETU

Konvencija o kibernetičkom kriminalitetu potpisana u studenom 2001., dokument je kojim je Vijeće Europe pokušalo dati smjernice u borbi protiv računalnog kriminala, pogotovo onog vezanog uz Internet. U listopadu 2005., stanje Konvencije je slijedeće:

Konvenciju je potpisalo preko trideset zemalja, a sada je ratificirana od strane jedanaest država članica Vijeća Europe (potpisnice koje su Konvenciju ratificirale u vrijeme nastanka prvog Prikaza bile su Hrvatska, Estonija i Albanija). Najavljeno je kako se ratifikacija Japana očekuje u toku mjeseca studenog 2005., čime će Japan postati prva zemlja izvan kruga zemalja članica Vijeća Europe koja će potpisanu Konvenciju uključiti u svoj pravni sustav.

Konvencija je stupila na snagu potpisivanjem od strane pet država, od kojih su tri trebale biti članice Vijeća Europe. Ovaj događaj zbio se 1. srpnja 2004., nakon ratifikacija Litve i Rumunjske. Sada se već slobodno može reći da je Konvencija postigla uspjeh, iako ratifikacija jedva da prelazi 30% zemalja potpisnica. Naime, cilj ovakvih Konvencija kao i mnogih tzv. "model" zakona kakve izrađuju, primjerice, Ujedinjeni Narodi prvenstveno je uvesti određene standarde – što se na području kaznenog prava i *cybercrimea* nesumnjivo i dogodilo. Za ilustraciju, UNCITRAL (United Nations Commission on International Trade Law) izradio je desetine model propisa koji, cijeli ili pojedine odredbe, danas upotpunjuju pravne sustave više od stotinu članica UN.

1. Temeljne odredbe Konvencije o kibernetičkom kriminalitetu

Konvencija definira po grupama inkriminacije vezane uz Internet, redom:

- grupu djela protiv tajnosti, nepovredivosti i dostupnosti podataka spremljenih na računalima i samih sustava (ovdje spadaju takve povrede kao što su neovlašten pristup računalu, neovlašteno presretanje podataka, neovlašteno mijenjanje i uništavanje podataka,

zloupotreba računala i programa radi počinjenja kažnjivih djela, ometanje nesmetanog rada računala itd.)

- kaznena djela poput prijevare i krivotvorenja uz pomoć računala
- kaznena djela vezana uz sadržaj podataka na računalima, prvenstveno uz posjedovanje i širenje dječje pornografije
- djela vezana uz kršenje autorskih i srodnih prava

Nakon samih kaznenih djela slijede i odredbe o:

- sankcioniranju pomaganja i prikrivanja pri izvršenju gore navedenih kaznenih djela (čl. 11)
- kaznenoj odgovornosti pravnih osoba za navedena kaznena djela (čl. 12)
- dužnosti zemalja potpisnica da u svoj kaznenopravni sustav unesu odredbe koje će osigurati da kaznena djela mogu biti kažnjavana s efektnim kaznama, uključivši i kaznu zatvora.

Na nekoliko mjesta u Konvenciji spominje se obveza zemalja potpisnica da u svoj pravni poredak unesu i odredbe koje će omogućiti i pristup i pretragu podataka na računalima korisnika osumnjičenih za počinjenje neke od inkriminacija gore opisanih, a koje su sadržane u odredbama članaka 2. do 10. Poseban je naglasak stavljen i na omogućavanje suradnje između zemalja potpisnica u vezi s istražnim radnjama. To je pogotovo očito u odredbama čl. 35 koji određuje dužnost zemalja potpisnica da osnuju službu koja će biti 24 sata na raspolaganju ako se pojavi potreba za suradnjom glede nadgledanja prometa na dijelu mreže u nadležnosti neke od zemalja potpisnica.

2. Kaznena djela protiv tajnosti, nepovredivosti i dostupnosti podataka spremljenih na računalima i samih računala – čl. 2 do čl. 6 Konvencije

1. Kazneno djelo neovlaštenog pristupa (Illegal Access, čl. 2)

2. Kazneno djelo neovlaštenog presretanja podataka (Illegal Interception, čl.3)
3. Kazneno djelo mijenjanja sadržaja, brisanja ili oštećenja podataka (Data Interference, čl.4)
4. Kazneno djelo ometanja normalnog rada računala (System Interference, čl. 5)
5. Kazneno djelo proizvodnje, prodaje, distribucije ili upotrebe uređaja dizajniranih u svrhu počinjenja nekog od prethodno navedenih kaznenih djela (Misuse of devices, čl. 6)

Kod definicije kaznenog djela neovlaštenog pristupa Konvencija kao sastavne dijelove dispozicije navodi namjeru počinjenja, bilo da je za cilj počinitelj imao neovlašteno pribavljanje podataka ili neku drugu nedopuštenu radnju.

Kazneno djelo neovlaštenog presretanja podataka definirano je kao namjerno bespravno presretanje privatnih emisija podataka, uključivši i nedopušteno praćenje elektromagnetskih emisija. U članku 3. ostavljena je mogućnost da država potpisnica u dispoziciju kaznenog djela ugradi uvjet postojanja nedopuštene namjere.

Kazneno djelo mijenjanja sadržaja, brisanja ili oštećenja podataka sastoji se od namjernog i bespravnog oštećenja, mijenjanja, brisanja podataka. Država stranka Konvencije može zadržati pravo da u dispoziciju kaznenog djela uključi uvjet da navedeno ponašanje treba rezultirati ozbiljnom štetom da bi bilo kaznenopravno sankcionirano.

Kazneno djelo ometanja normalnog rada računala pokriva sve oblike bespravnog namjernog ometanja rada računala, bilo kroz oštećenje ili brisanje podataka na računalu ili emitiranjem podataka (DoS i DDoS napadi) s drugog računala.

Kazneno djelo proizvodnje, prodaje, distribucije ili upotrebe uređaja dizajniranih u svrhu počinjenja nekog od prethodno navedenih kaznenih djela odnosi se kako na uređaje, hardver, tako i na različite maliciozne programe poput kompjuterskih virusa i trojanskih konja. Interesantno, u dispoziciju kaznenog djela uključeno je i posjedovanje lozinki (zapravo, backdoor-ova) koji bi mogli omogućiti neovlašteni pristup, naravno uz postojanje namjere da se počini neko od gore navedenih kaznenih djela. U slučaju da ne postoji takva namjera, tada neće biti riječ o kaznenom djelu.

Kod svih kaznenih djela iz ove glave postojanje namjere je ključno za postojanje bića kaznenog djela. Primjetno je i relativno blago formiranje dispozicija kaznenih djela uz brojne mogućnosti da države stranke izjave rezerve.

3. "Uobičajena" kaznena djela počinjena pomoću računala

U ovoj glavi, koja pokriva članke 7. i 8., navedena su dva uobičajena kaznena djela počinjena pomoću računala:

1) Kazneno djelo krivotvorenja
2) Kazneno djelo prijevare

Riječ je o kaznenim djelima kod kojih, naravno, biće kaznenog djela postoji neovisno o tome da li je kazneno djelo počinjeno pomoću računala ili nije, za razliku od kaznenih djela iz prethodne glave kod kojih je upotreba računala jedno od temeljnih obilježja i uvjet sine qua non.

Kod kaznenog djela krivotvorenja, kao elementi dispozicije navedeni su namjera, te bespravno oštećenje, brisanje ili izmjena podataka sa svrhom da se ti podaci smatraju ispravnima i zakonski važećima da bi se stekla neka protupravna korist.

Kod kaznenog djela prijevare počinjene pomoću računala u dispoziciju je uključena i mogućnost počinjenja pomoću unosa, izmjene, brisanja i oštećenja podataka kao i svako drugo utjecanje na normalan rad računala. I kod ovog kaznenog djela sastavni dio dispozicije je namjera stjecanja protupravne imovinske koristi.

4. Kaznena djela vezana uz sadržaj (kaznena djela vezana uz dječju pornografiju, povrede autorskog i srodnih prava)

Konvencija u čl. 9. traži od svake zemlje potpisnice da usvoji legislativu potrebnu za inkriminaciju distribucije dječje pornografije putem kompjutorskih sustava. Kažnjivo je postavljanje takvih podataka na računalne sustave s kojih bi mogli biti ponuđeni na Internet, čuvanje podataka koji sadrže dječju pornografiju na kompjutorskim sustavima i medijima za pohranu podataka, pribavljanje dječje pornografije pomoću kompjutorskog sustava za sebe ili drugog, kao i samo kreiranje podataka sa takvim sadržajem sa svrhom distribucije kroz kompjutorski sustav.

Konvencija ovdje i definira dječju pornografiju iako ostavlja rezervu potpisnicama da same urede dob maloljetnika snimanje čijeg seksualno eksplicitnog ponašanja se smatra dječjom ponografijom (Konvencija postavlja granicu na 18 god, ali dopušta potpisnicama snižavanje do 16 g).

Konvencija u čl. 10. navodi obvezu svake zemlje potpisnice da usvoji legislativu kojom bi se ustanovio pravni okvir za kažnjavanje kršenja autorskih prava počinjenim pomoću kompjutorskog sustava (uz zakonodavstvo države potpisnice vezano za zaštitu autorskog i srodnih prava, upućuje se i na **odredbe Bernske Konvencije za zaštitu literarnih i umjetničkih djela** s **Pariškim dodatkom** od 24. lipnja 1971. kao i na odredbe **WIPO Povelje o autorskim pravima** (World Intellectual Property Organization).

VII. PRILOG - OSVRT NA ODGOVORNOST PRUŽATELJA INTERNET USLUGA (ISPa)

Internet je područje u kojem se danas isprepliću ozbiljni poslovni interesi i zahtjevi za poštovanjem privatnosti, tajnosti i nepovredivosti osobnog komuniciranja s jedne strane, i brojne mogućnosti zloupotrebe. Pravno gledano, još uvijek postoje brojne pravno neregulirane ili konfliktno regulirane sive zone, pogotovo u odnosima različitih pravnih poredaka. Pristup kontroli sadržaja na Internetu također je različit ovisno o pravnom sustavu koji je nositelj kontrole. Kontrola sadržaja svakako je blaža u zemljama zapadne europsko američke kulture, dok mnoge islamske i azijske zemlje imaju striktne propise o zabranjenim sadržajima na serverima koji pripadaju pod njihovu nadležnost. Neke od tih zemalja, poput Irana i Kine, idu toliko daleko da osim kontrole sadržaja na serverima na vlastitom teritoriju i u vlastitim nacionalnim domenama, filtriraju promet vlastitih korisnika prema serverima u drugdje u svijetu

U vrijeme nastanka Interneta, odnosno evolucije iz nekadašnjeg američkog ARPANeta (Advanced Research Projects Network američkog ministarstva obrane) računala – serveri bila su smještena po ustanovama članicama ARPANet-a, prvenstveno vojnim, a zatim i sveučilišnim.

Početkom devedesetih godina dvadesetog stoljeća započela je komercijalizacija Interneta i pojavili su se prvi privatni pružatelji Internet usluga, kako spajanja na Internet (dial-up i leased line) tako i pružanja prostora na računalima (web hosting). Takve pravne osobe, dionička društva ili društva s ograničenom odgovornošću, poznate su pod američkim nazivom ISP/IPP (Internet Service Provider/ Internet Presence Provider – pružatelj Internet usluga / usluga smještaja web stranica). Neke od tih tvrtki su se na pružanje Internet usluga prebacile sa pružanja različitih BBS[41] usluga, dok su druge bile sasvim nove tvrtke. U ovom trenutku, postoji više od dvije tisuće različitih pružatelja Internet usluga širom svijeta. Velika većina njih svoju djelatnost bazira na nekoliko osnovnih usluga o kojima je već iznad bilo nešto riječi:

[41] bulletin board system, vrsta jednostavnije računalne mreže popularne u Sjedinjenim državama i Zapadnoj Europi krajem sedamdesetih i početkom osamdesetih godina dvadesetog stoljeća

- **Omogućavanje spajanja klijenata na Internet**
- **Pružanje usluge smještaja web-stranica i podataka**
- **Različiti oblici edukacije i popularizacije korištenja Interneta**

Kad korisnici koriste usluge ISP tvrtke postoji mogućnost da će neki od njih počiniti i neki od pojavnih oblika računalnog kriminaliteta, pogotovo onih koji cvjetaju na Internetu. Zbog toga mnoge ISP tvrtke imaju organiziranu službu koja zaprima i obrađuje prijave različitih sigurnosnih incidenata vezanih uz korisnike koji koriste njihove usluge i imaju mogućnost takvim korisnicima uskratiti daljni pristup. Takve službe (često nazvane "abuse" službama) u načelu surađuju sa istovrsnim službama drugih ISPova radi sprečavanja incidenata širih razmjera, poput DDOS napada (više o tome infra).

Tako danas imamo dvije glavne kategorije ISPova, privatne tvrtke (npr. u Hrvatskoj to su Iskon Internet, GlobalNet, VIPNet i naravno T-com, da nabrojimo samo poznatije) te različite ustanove poput vojske i obrazovnih institucija širom svijeta (kod nas CARNet, Hrvatska akademska i istraživačka mreža). Načelno svi ISP-ovi imaju organiziranu službu za zaprimanje i obradu sigurnosnih incidenata s ovlastima da upozori korisnike-počinitelje i uskrati im dalji pristup u cilju očuvanja sigurnosti svoje mreže i Interneta u cjelini.

Međunarodno i komparativno pravo

U zadnjih nekoliko godina u svijetu je na snagu stupilo ili je u postupku stupanja na snagu nekoliko propisa koji se uz ostala pravna pitanja vezana uz Internet i moderne informacijske i telekomunikacijske tehnologije bave odgovornošću tvrtke pružatelja pristupa (ISP/IPP) Internetu.

Iz hrvatske perspektive svakako posebno mjesto zaslužuje **Cybercrime Convention – Konvencija o kibernetičkom kriminalu** potpisana u Budimpešti 23. studenog 2001.

1997. Doneseni njemački propisi **Teledienstgesetz – TDG** (Zakon o telekomunikacijskim uslugama) i **Mediendienstestaatsvertrag – MDStV** također su važni s hrvatske točke gledišta.

Treći veliki utjecaj na hrvatski pravni sustav svakako je i francusko pravo, a relevantan izvor prava u ovom slučaju je Zakon o emitiranju audiovizualnih sadržaja od 20. rujna 1986. dopunjen odgovarajućim amandmanima 1998. (**Ammendment Fillon**, po tadašnjem ministru zaduženom za telekomunikacije, od kojih su dva kasnije srušena nakon što je grupa senatora predložila francuskom tijelu nadležnom za ispitivanje ustavnosti zakona ("Conseil Constitutionnel") da ispita usklađenost tih, od mnogih okarakteriziranih kao brzopleto donesenih, amandmana).

Naravno, tu je i austrijsko pravo te osvrt na rad dr. Gabrielle Schmölzer posvećen Internetu i kaznenom pravu[42] u kojem ona poseban naglasak stavlja na kaznene odredbe austrijskog Kaznenog zakona (St.G.B.) i Zakona o kaznenom postupku (St.P.O).

Odredbe Konvencije o kibernetičkom kriminalu u pogledu odgovornosti ISP

Tekst Konvencije, nakon Preambule, definira osnovne pojmove kojima se Konvencija bavi. U članku 1. st. 1. nalazi se važna definicija pružatelja usluga, "service providera". [43] Ova prilično široka definicija utvrđuje da je pružatelj usluga svaka privatna pravna osoba ili ustanova koja svojim korisnicima pruža mogućnost komuniciranja pomoću računalnog sustava, te bilo koje drugo tijelo koje pomaže pri obradi ili skladištenju tako stečenih podataka u ime i za račun korisnika.

Za ovaj pregled svakako je najvažniji članak 12. st. 2. koji se bavi odgovornošću pravnih osoba. Konvencija jasno zahtijeva poduzimanje svih potrebnih radnji da se u pravni poredak država potpisnica unesu odredbe koje omogućuju vođenje postupka jednako protiv fizičkih kao i protiv pravnih osoba, kako privatnih tako i ustanova i državnih organizacija. Ovisno o prirodi počinjenog djela traži se

[42] Dr.sc. Gabrielle Schmölzer: "Internet und Straffsrecht", "Straffrechtliche Probleme der Gegenwart", cl . 25 1998.

[43] ovdje prenesena u cijelosti:
"Service provider means:
i. any public or private entity that provides to users of its service the ability to communicate by means of a computer system, and
ii. any other entity that processes or stores computer data on behalf of such communication service or users of such service."

mogućnost postojanja kaznene, građanske i upravno-pravne odgovornosti, kako za zaposlenike tako i za same pravne osobe.

Cybercrime Konvencija je definitivno ostvarenje jednog od raisons d'ētre Vijeća Europe, a to je rad na ujednačenju legislative članica i pripremu njihovih pravnih poredaka za budućnost u Europskoj Uniji. Njezine su odredbe definitivno u duhu s vremenom, no pravni poredak većine zemalja je definitivno konzervatoran, rijetko kad kreatoran, i kreće se po vlastitoj inerciji.

Konvencija sadrži priličan broj rezervi (članci - odredbe Konvencije koje se mogu, ali i ne moraju prihvatiti od strane država potpisnica. Države potpisnice mogu izrijekom izjaviti neku od rezervi koja se tada neće primijenjivati u njihovom pravnom sustavu) koje je moguće u bilo koje vrijeme notifikacijom istaknuti (čl. 42.). Bit će prilično teško pratiti u kojem je trenutku koja zemlja potpisnica istaknula ili povukla koju od rezervi (a ima ih desetak). Toga su definitivno svjesni i u tijelima Vijeća Europe pa su na na web stranicama Vijeća Europe posvećenim Konvenciji postavili tablicu potpisa i ratifikacije, te mogućnost oznake istaknutih rezervi za svakog od potpisnika.

Komparativno pravo – Francuska

Kao jedna od vodećih zemalja kontinentalnog pravnog kruga, ali i tehnološki avangardna nacija, Francuska se rano susrela s problemom regulacije odgovornosti ponuđača Internet usluga. Put kojim je francuski pravni sustav krenuo sastoji se u razlikovanju uloge tvrtke kao pružatelja usluge spajanja na Internet i uloge pružatelja prostora na poslužiteljima koji će nuditi svojim korisnicima mogućnost da postave svoje sadržaje u obliku web stranica, datotečnih repozitorija ili oglasnih ploča (foruma).[44]Krajem devedesetih dogodio se niz slučajeva u kojim su razna tijela zauzimala različite stavove, (Union des Etudiants Juifs de France vs. Compuserve, zatim Francuska protiv FranceNet i WorldNet) no konačan zaključak koji je proizašao slijedi. Tvrtke koje se bave pružanjem usluge spajanja na Internet nisu u mogućnosti pratiti sav promet koji prolazi njihovim računalima.

[44] Vallerie Sedallian : " Controlling Illegal Content over the Internet", izlaganje održano u toku 26. International Bar Association Conference u Berlinu, 1996.

Kako francusko kazneno zakonodavstvo traži za djela počinjena pomoću računala namjeru, to tvrtke pružatelji usluge spajanja na Internet nisu i ne mogu biti kazneno niti građanskopravno odgovorne. Što je s tvrkama koje pružaju uslugu prostora na web poslužiteljima? Ako je tvrtka pružatelj upoznata s prijestupom, i ne poduzme mjere u njenoj mogućnosti da spriječi širenje kažnjivog sadržaja, tada bi mogla biti odgovorna. Gore navedeni **Amendments Fillon** su dodali dvije obveze za tvrtke pružatelje Internet usluga. Tvrtke pružatelji su dužne svojim korisnicima pružiti programe s mogućnošću kontrole pristupa (**parental lock**), te blokirati pristup web-stranicama i drugim Internet sadržajima koji sadrže materijale koji se mogu podvesti pod neku od inkriminacija iz korpusa francuskog kaznenog prava, u ovom slučaju sadržanog u odredbama kaznenog zakonika i već navedenog Zakona o emitiranju audiovizualnih sadržaja sa pripadajućim amandmanima.

Komparativno pravo – Njemačka

I prije nego je **Teledienstgesetz – TDG,** odnosno Zakon o telekomunikacijama, donesen, njemačko je pravosuđe zauzelo sličan stav o odgovornosti proizvođača kakav je prevalentan i u francuskom pravnom poretku. Zbog nehaja, pružatelj Internet usluga ne može biti kažnjen. I njemački se zakonodavac ovdje poziva na prirodu i tehničku stranu posla tvrtke pružatelja usluga koja onemogućuje pružatelja usluga da bude svjestan sadržaja svih informacija prenesenih od strane korisnika njegove usluge. Slično poput bilo kojeg telekoma, uloga pružatelja usluga je samo prenositi informacije, on ne treba biti svjestan njihovog sadržaja. Ovdje sad dolazimo i do dihotomije sadržane u njemačkom pravu u vezi ovog konkretnog slučaja. Naime, izgleda da savezni zakon, **TDG**, odstupa od normi sadržanih u **Mediendienststaatsvertrag – MDStV** kao izrazu zakonodavne volje njemačkih saveznih država (Ländern). Riječ je o dužnosti pružatelja usluga da, ako zna za postojanje nelegalnog sadržaja i ako je onemogućivanje sadržaja za njega tehnički izvedivo (a da ne ugrozi svoje dužnosti prema svojim drugim klijentima), onemogući zabranjen sadržaj. **MDStV** s druge strane traži obvezu blokiranja saržaja ako to zatraži njemački organ nadležan za brigu i prava mladeži, ekvivalentan našem Centru za socijalnu skrb.

I njemački sustav građanskopravne i kaznene odgovornosti razlikuje pružatelja Internet pristupa i pružatelja usluga smještaja web stranica. Za razliku od francuskog pristupa i pristupa iz Cybercrime Konvencije, načelno je kroz opće propise bila predviđena, osim odgovornosti za namjeru, i odgovornost za nehaj (negligence). Ipak, i ovdje je prisutna bojazan da je efektivna kontrola i svijest pružatelja usluge o sadržaju zbog ogromne količine informacija praktično nemoguća, pa su i **TDG** i **MDStV** isključili nehaj i koncentrirali se samo na namjeru. Tvrtka pružatelj usluga može biti odgovorna ako je svjesna sadržaja. U njemačkoj se sudskoj praksi zatim postavilo pitanje kada se može reći da je tvrtka svjesna sadržaja, i da li svjesnost nekog u nekom ogranku tvrtke tereti i centralu, odnosno postoji li odgovornost centrale tvrtke ako postoji saznanje da je netko od zaposlenih u nekoj od podružnica bio svjestan nelegalnog sadržaja. Federalni sudovi našli su da u ovom slučaju odgovornost centralnih organa tvrtke postoji. Svako saznanje unutar tvrtke o sadržaju dovoljno je da postoji odgovornost tvrtke za sadržaj koji se putem njezinog servera nudi.

Dakle, njemačko pravo smatra da ne postoji odgovornost pružatelja usluga spajanja (access provider), zato što po čl. 13 njemačkog kaznenog zakonika ne postoji dužnost pružatelja, obveza za pružatelja, da pazi na sadržaj koji se emitira kroz njegovu opremu na Internet. [45]

Što se tiče odgovornosti pružatelja usluga smještaja web stranica, ona postoji ako postoji namjera.

Komparativno pravo – Austrija

U austrijskom pravnom sustavu, odredbe o odgovornosti pružatelja Internet usluga sadržane su u :

- **Kaznenom zakoniku (St.GB)**
- **Zakonik o kaznenom postupku (St.PO)**
- **Telekomunikationsgesetz**
- **Zakon o tisku i drugim sredstvima javnog pripoćavanja (1993.)**
- **I nekim drugim, usko specijaliziranim zakonima**

[45] Prof. Dr. Ulrich Sieber : Responsibility of Internet Providers, str. 9

I austrijski sustav smatra da se načelno ne može smatrati odgovornim pružatelja usluge pristupa Internetu. Što se tiče pružatelja usluge smještaja web stranica opskrbljivač, service – provider, može se osloboditi odgovornosti ako je primijenio dužnu pažnju[46].

S time se slaže i Sieber koji navodi još jedan primjer iz čl. 75. i čl. 104. st.1 **Telekomunikationsgesetz** gdje načelno postoji odgovornost pružatelja usluga, ali se izrijekom pružatelji usluge spajanja na Internet izuzimaju iz generalne odgovornosti pa tako izlazi da tvrtke vlasnici opreme za pružanje Internet usluga ne mogu biti odgovorni za njenu zloupotrebu u smislu počinjenja kaznenih djela i prekršaja.[47]

G. Schmölzer također u svom djelu o odnosu kaznenog prava i Interneta navodi i odredbe austrijskog pravnog poretka o odgovornosti za širenje nacional-socijalističke literature i ideja, inkriminacija po **Zakonu o zabrani Nacionalsocijalističke njemačke narodne stranke** iz 1945, noveliranog 1952.

U austrijskom pravnom sustavu postoji svijest o kažnjavanju tvrtki pružatelja usluga koji znaju za nedopušten sadržaj na njihovim računalnim sustavima, a ne poduzimaju ništa da se promet takvog sadržaja blokira. S druge strane, ako tvrtke pružatelji usluga nisu svjesne postojanja takvog sadržaja, što zbog obima prenesenih informacija nije nezamislivo, tada načelno ne postoji njihova odgovornost[48]. Po mišljenju G. Schmölzer, Austriji tu još treba jasno zakonsko utvrđivanje dužnosti nadzora i njenih daljih učinaka.

Komparativno pravo – SAD

U SAD, odgovornost pružatelja Internet usluga regulirana je slijedećim propisima:

- **Communications Decency Act**
- **Child Online Protection Act**
- **Online Copyright Infrigement Liability Limitation Act kao dio Digital Milennium Copyright Protection Act-a**

[46] Gabrielle Schmölzer : Internet i kazneno pravo, prijevod u Hrvatskom ljetopisu za kazneno pravo vol.4 2/97, str. 895.
[47] Prof. Dr. Ulrich Sieber : Responsibility of Internet Providers, str. 14

Prvi po redu, **Communications Decency Act** smatra da ne postoji odgovornost pružatelja usluge ako on samo pruža uslugu pristupa, ili korisnicima pruža softver koji omogućuje pristup, ili održava sustave vezane uz tehničko funkcioniranje Internet veze (Proxy sustavi, DNS sustavi). Naravno, odsustvo odgovornosti ne postoji kada pružatelj usluge surađuje sa autorima nezakonitog sadržaja, ili je svjestan postojanja takvog sadržaja, ali ne čini ništa da ga ukloni[49].

Kad je 1998. na snagu stupio **Child Online Protection Act**, pružatelji Internet usluga postali su zakonom obvezni da obavijeste svoje korisnike prilikom sklapanja ugovora da postoji softver s mogućnošću filtriranja sadržaja. Isto tako, taj je propis donio i odredbu kojom su odgovorni oni koji učine dostupnim preko Interneta sadržaj koji je štetan djeci i maloljetnicima. Ta odgovornost opet ne odnosi se na pružatelje samog pristupa već one koji smještaju takav sadržaj na svoje stranice. Takvi se pružatelji usluga mogu ograditi od odgovornosti tako da zaštite takve stranice obveznom upotrebom identifikatora i lozinki, te obaviješću kako je riječ o stranicama zabranjenim za maloljetnike.

Online Copyright Infringement Liability Limitation Act iz 1998. sadrži odredbe glede odgovornosti i ograničenju odgovornosti pružatelja Internet usluga za objavljivanje nedozvoljeno umnoženog ili drugog materijala koji krši autorska i srodna prava. Ograničenje odgovornosti odnosi se na slučaj kada pružatelj usluga na osnovu informacija o postojanju materijala koji krši autorska i srodna prava bez zadrške blokira pristup i odstrani takav sadržaj sa servera pod svojom nadležnošću. Ovaj propis također specificira prilično formalan postupak kako se može od tvrtke pružatelja usluge zahtijevati skidanje i blokiranje pristupa sadržaju koji vrijeđa autorska i srodna prava. Prvenstveno se od tvrtke pružatelja usluga traži da imenuje "designated agent", osobu određenu da prima zahtjeve za odstranjenje određenog sadržaja. Od strane koja smatra da su joj prava povrijeđena traži se:

1) potpisani zahtjev kojim se traži odstranjenje spornog materijala

[48] Gabrielle Schmölzer : Internet i kazneno pravo, prijevod u Hrvatskom ljetopisu za kazneno pravo vol.4 2/97, str. 897
[49] Prof. Dr. Ulrich Sieber : Responsibility of Internet Providers, str. 17

2) dovoljno podataka da se može ustanoviti o povredi prava kojeg djela je riječ
3) potrebni podaci da pružatelj usluga može ustanoviti koji je materijal objavljen putem njegovog računalnog sustava sporan
4) osobni podaci tužitelja da pružatelj usluge može s njim stupiti u kontakt
5) izjavu da kao tužitelj nastupa u dobroj vjeri da posjeduje prava čiju zaštitu traži[50]

Naravno, sličnim je postupkom regulirano i pravo onog koji je sporni sadržaj stavio na Internet da reagira na zahtjev oštećenika, pa i da istim putem zatraži ponovno postavljanje sadržaja na Internet i omogućavanje pristupa ako se pokaže da nije došlo do povreda navedenih od strane navodnog oštećenika.

Nadalje, zakon jasno kaže da ne postoji obveza na strani pružatelja usluge da aktivno prati i evaluira sadržaj objavljen na svojim serverima u potrazi za sadržajem koji bi mogao biti protivan odredbama o zaštiti autorskih i srodnih prava.

Sieber dalje smatra da je američki zakonodavac ovim propisom uspostavio izbalansirani kompromis između interesa nosioca autorskih i srodnih prava čija bi prava mogla biti ugrožena i pružatelja usluga. Posebni problemi koji se javljaju kod utvrđivanja odgovornosti kod primjene informatičkih sustava dobili su specijalne odredbe. Takav sustav potiče suradnju nositelja autorskih prava i pružatelja Internet usluga, i isto tako daje poticaj za unapređenje tehničkih sredstava u vezi s tim.[51]

[50] Prof. Dr. Ulrich Sieber : Responsibility of Internet Providers, str. 19
[51] Prof. Dr. Ulrich Sieber : Responsibility of Internet Providers, str. 20

VIII. ZAKLJUČAK

Pojavni oblici kompjutorskog kriminaliteta zastupljeni su u većoj ili manjoj mjeri u svim zakonodavstvima izabranima za ovaj pregled. To i ne čudi, uzme li se u obzir činjenica da sve veći postotak njihovih ekonomija ovisi o računalnoj tehnologiji, povećavajući efikasnost proizvodnje, ali i istovremeno stvarajući podesan teren za neka društveno neprihvatljiva ponašanja. Kako pravo uvijek prati razvitak društva, pa tako i gospodarstva, očigledna je veza naprednog gospodarstva i visokog nivoa zastupljenosti pojavnih oblika kompjutorskog kriminaliteta u kaznenopravnim sustavima zemalja. Tako gospodarski napredne zemlje s visokim stupnjem Internet penetracije, poput SAD, Francuske i Njemačke, sasvim očekivano prednjače i zakonodavnim rješenjima i praksom, a njima se u posljednje vrijeme približio i Japan, koji je u prethodnom pregledu priredio svojevrsno iznenađenje nešto slabijom «opremljenosti» zakonodavstva.

Kako su statistike pokazale, nimalo laskavu titulu zemlje s najvišom stopom kibernetičkog kriminaliteta već nekoliko godina nosi Brazil, što je bio i poticaj da se stekne uvid u brazilsko zakonodavstvo i istraže uzroci takvog stanja. Osim Brazila, slični trend možemo zapaziti i u Indiji i Turskoj, koje s Brazilom dijele brzo širenje novih informacijskih tehnologija i nedostatnu opremljenost i osposobljenost zakonodavstva i pravosudnih organa.

Zemlje naše neposredne okoline, nastale raspadom bivše zajedničke države, uključivši i Hrvatsku, učinile su posljednjih godina mnogo u usvajanju potrebne legislative. Slovenija, kako je već navedeno i u izvješću BSA, prednjači visokom razinom borbe protiv piratstva, koje je još uvijek u Hrvatskoj i drugim zemljama sljednicama SFRJ prilično rašireno. Konkretan dokaz ovoj tvrdnji su nedavna izvješća BSA za nekoliko zemalja regije kojima se te zemlje (savim očekivano) svrstavaju u vrh europskih zemalja po raširenosti piratiziranog softvera, premda posjeduju sasvim moderna zakonska rješenja za borbu protiv piratstva i drugih oblika kompjutorskog kriminaliteta.

U ovom trenutku većina zemalja posjeduje ili će uskoro posjedovati potreban zakonski okvir za borbu protiv cybercrimea, no ono što još uvijek ne ohrabruje jest

organizacija službi unutar i izvan policijskih snaga i drugih organa reda u navedenim zemljama koje bi trebale biti najistureniji državne ustanove u borbi s informatičkim kriminalom. Dok napredne zapadne zemlje imaju sve više različitih službi koje se bave ovim problemom, pa se čak javljaju (posebno u posljednje vrijeme, zbog svjetske sigurnosne situacije i prijetnje od terorističkih napada) udruge građana koje prosvjeduju protiv sve većeg zadiranja u privatnost, neke od gore navedenih zemalja zapravo niti nemaju pravu ustanovu ili drugu službu koja bi surađivala sa policijom i oštećenima radi otkrivanja počinitelja.

Naravno, i u Hrvatskoj i okolnim zemljama javlja se i pitanje obrazovanosti i osposobljenosti. Nedavno prihvaćeni Nacionalni program informacijske sigurnosti sadrži opsežan paket mjera koje će, budu li provedene kako je zamišljeno, vrlo pozitivno utjecati na izgradnju informacijskog društva u Republici Hrvatskoj.

DODATAK:
Tablica 1.

	KAZNENA DJELA PO KONVENCIJI O KIBERNETIČKOM KRIMINALITETU* Kaznena djela vezana uz integritet podataka, pristup računalima i neometano funkcioniranje računala				
ZEMLJE:	**Illegal Access čl. 2**	**Illegal Interception čl.3**	**Data Interference čl.4**	**System Interference čl. 5**	**Misuse of devices čl. 6**
Njemačka	√	√	√	√	√
Austrija	√[52]	√	√	√	√
V. Britanija	√	√	√	√	√
SAD	√	√	√	√	√
Francuska	√	√	√	√	√
Švedska	√	√	√	√	√
Japan	√	√	√	√	√
Kina	√	√	√	√	√
Brazil	X	X	√	√	X
Srbija i CG	√	√	√	√	√
Slovenija	√	√	√	√	√
Hrvatska	√	√	√	√	√

Tablica 1. – Listopad 2005. - Kaznena djela protiv tajnosti, nepovredivosti i dostupnosti podataka spremljenih na računalima i samih računala – čl. 2 do čl. 6 Konvencije

1. Kazneno djelo neovlaštenog pristupa (Illegal Access, čl. 2)
2. Kazneno djelo neovlaštenog presretanja podataka (Illegal Interception, čl.3)
3. Kazneno djelo mijenjanja sadržaja, brisanja ili oštećenja podataka (Data Interference, čl.4)
4. Kazneno djelo ometanja normalnog rada računala (System Interference, čl. 5)

[52] Regulirano austrijskim **Zakonom protiv nelojalne konkurencije**

5. Kazneno djelo proizvodnje, prodaje, distribucije ili upotrebe uređaja dizajniranih u svrhu počinjenja nekog od prethodno navedenih kaznenih djela (Misuse of devices, čl. 6)

IX. LITERATURA

1. Doc.dr.sc. Dražen Dragičević: "Kompjutorski kriminalitet i informacijski sustavi", Informator Zagreb, 1999.
2. Prof. Dr. Ulrich Sieber : Responsibility of Internet Providers, **http://www.iura.uni-muenchen.de/sieber**, University of Würzburg
3. Gabrielle Schmölzer : Internet i kazneno pravo, prijevod u Hrvatskom ljetopisu za kazneno pravo vol.4 2/97, str. 891.-897.
4. Vallerie Sedallian : " Controlling Illegal Content over the Internet", izlaganje održano u toku 26. International Bar Association Conference u Berlinu, 1996.
5. Tihomir Katulić "Odgovornost pružatelja Internet usluga", Informator prosinac 2004
6. Tihomir Katulić "Sklapanje trgovačkih ugovora elektroničkim putem" siječanj 2005
7. http://www.usdoj.gov/criminal/cybercrime/fedcode.htm - popis federalnih propisa vezanih za kompjutorski kriminalitet.
8. Handbook of Legislative Procedures of Computer and Network Misuse in EU Countries for assisting Computer Security Incident Response Teams (CSIRTs)
9. http://www.isc.meiji.ac.jp/~sumwel_h/Codes/comp-crim.htm - zbirka relevantnih japanskih propisa
10. Tekst Zakona o autorskom pravu : **http://www.cric.or.jp/cric_e/clj/clj.html** - tekst japanskog zakona o autorskom pravu
11. **http://www.projuris.org/aktuelno_comp_kriminal.htm** članak o srpskom zakonodavstvu i komojutorskom kriminalitetu
12. Službeni glasnik Srbije SRS 80/2002 i 39/2003 – srpski Krivični zakon
13. Register predpisov Slovenije, Ur.l. RS, št. 23/99, čl.225 slovenski Kazenski zakonik
14. **http://www.aas.si/pravni-viri/kzrs-fr1.html** o zaštiti autorskih prava u slovenskom kaznenom zakoniku
15. **http://www.ekonomist.co.yu/magazin/ebit/12/por/slovenc.htm**
16. **http://www.sweden.gov.se/sb/d/3926/a/27777** - Švedski kazneni zakon

X. KATALOG HRVATSKIH PROPISA

1. Zakon o zaštiti osobnih podataka NN 106/2003
   http://www.nn.hr/clanci/sluzbeno/2003/1364.htm
2. Zakon o elektroničkoj trgovini NN 173/2003
   http://www.nn.hr/clanci/sluzbeno/2003/2504.htm
3. Zakon o telekomunikacijama NN 122/2003
   http://www.nn.hr/clanci/sluzbeno/2003/1731.htm
4. Zakon o elektroničkom potpisu NN 10/2002
   http://www.nn.hr/clanci/sluzbeno/2002/0242.htm
5. Zakon o autorskom pravu i srodnim pravima NN 167/2003
   http://www.nn.hr/clanci/sluzbeno/2003/2399.htm
6. Kazneni zakon
   http://www.nn.hr/clanci/sluzbeno/1997/1668.htm
   http://www.nn.hr/clanci/sluzbeno/2004/2026.htm
7. Zakon o kaznenom postupku
   http://www.nn.hr/clanci/sluzbeno/2003/0740.htm