HRVATSKA AKADEMSKA I ISTRAŽIVAČKA MREŽA
CROATIAN ACADEMIC AND RESEARCH NETWORK

PRIKAZ KAZNENOG ZAKONODAVSTVA S PODRUČJA KOMPJUTORSKOG KRIMINALITETA

CCERT-PUBDOC-2003-HH-LI

CARNet CERT

Sigurnosni problemi u računalnim programima i operativnim sustavima područje je na kojem CARNet CERT kontinuirano radi. Rezultat toga 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.

X¬«¦ℚ k ~¦ ¤ © bw«¬£ ĝ

Sadržaj

I. KONVENCIJA O KIBERNETIČKOM KRIMINALU

Konvencija potpisana u studenom 2001., dokument je kojim je Vijeće Europe pokušalo dati smjernice u borbi protiv računalnog kriminala, pogotovo onog vezanog uz Internet. Konvenciju je potpisalo preko trideset zemalja, a za sada je ratificirana od strane svega tri države (Hrvatska, Estonija i Albanija). Konvencija stupa na snagu kad ju potpiše barem pet država, od kojih barem tri trebaju biti članice Vijeća Europe.

Konvencija definira po grupama inkriminacije vezane uz Internet, pa redom imamo:

- 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 distribuciju 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 sa 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.

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) sa 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.

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.

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 sa Pariškim dodatkom od 24. lipnja 1971. kao i na odredbe WIPO Povelje o autorskim pravima (World Intellectual Property Organization).

II. PREGLED ZAKONODAVSTAVA DRŽAVA

Uvid u kaznenopravne sustave država na slijedećim stranicama koristan nam je da steknemo predodžbu o načinima na koje različiti pravni sustavi rješavaju problem inkriminacije ponašanja koja čine djela kompjutorskog kriminaliteta.

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

Prvenstveno, biti će obrađeni pravne sustave Njemačke i Austrije, kako zbog njihove gospodarske snage i 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 prirpadaju istom pravnom krugu. U zemlje kontinentalnog pravng kruga ubraja se i Francuska, za koju će se isto naći mjesta.

Pravni sustavi Velike Britanije i SAD svakako se trebaju naći u svakom komparativnom pregledu stranog prava. Riječ je o državama specifičnog, presedanskog (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 dobiti će 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 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

Kao što smo već naglasili, 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, a slijedećem tekstu pokušati ću na primjeru Njemačke pokazati drugi od navedenih pristupa.

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.[1]

Ipak, korpus modernog kaznenog prava u vezi sa kompjutorskim kriminalitetom svodi se u Njemačkoj na slijedeće pravne izvore:

- Drugi Zakon o spriječavanju 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)
- 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 sankcioniralo kaznena djela:

- samog neovlaštenog pristupa
- neovlaštenog korištenja kompjutorskog sustava za osobne potrebe (tzv. krađa vremena)[2]

[1] Doc.dr.sc. Dražen Dragičević, "Kompjutorski kriminalitet i računalni sustavi", str 171
[2] Doc.dr.sc. Dražen Dragičević, "Kompjutorski kriminalitet i računalni sustavi", str 176

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 sa 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.

Ako sad usporedimo njemačko zakonodavstvo sa smjernicama zadanim u Konvenciji o kibernetičkom kriminalu, vidimo da je u velikoj mjeri već sad njemačko zakonodavstvo usuglašeno sa relevantnom europskom legislativom. Nadalje, njemački sudovi imaju značajno, gotovo tridesetogodišnje iskustvo u rješavanju slučajeva vezanih za kompjutorski kriminalitet. Kada Konvencija o kibernetičkom kriminalu bude konačno stupila na snagu, Nijemcima preostaje još kaznenopravno sankcionirati sam neovlašteni pristup, kao i možda malo detaljnije zaštititi pravilno funkcioniranje računala u smislu kažnjavanja različitih denial of service napada. Premda se to može podvesti pod ometanje normalnog rada sustava koje već postoji kao inkriminacija u gorenevedenom Drugom Zakonu o spriječavanju gospodarskog kriminaliteta, odnosno njime nadopunjenom njemačkom Kaznenom zakonu, u novije vrijeme DoS i DDos napadi imaju sve veću težinu i opasnost za pravilno funkcioniranje Interneta, a time i potencijal za nanošenje ozbiljne gospodarske štete.

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.[3] 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.

Takvo neodrživo stanje dovelo je do reforme kaznenog zakonodavstva. 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.

Nažalost, prijedlog je samo djelimično prihvaćen, tako da su konačnu novelu Strafgesetzbucha unešena samo kaznena djela oštećenja podataka (čl. 126 StGB) i prijevarne zloupotrebe obrade podataka (čl. 148 StGB). Novi je Kazneni zakon stupio na snagu 1988.

1. Kazneno djelo oštećenja podataka (čl.126 StGB)

Za razliku od nekih drugih zemalja, koje su posebno inkriminirale kompjutorsku sabotažu, poput Njemačke, Japana, Brazila, Poljske i Kanade[4], 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 zaprijećena je i viša kazna (čl. 126a st.2.)

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

2 . Kazneno djelo prijevarne zloupotrebe obrade podataka (čl. 148a)

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).

Ono što iznenađuje u austrijskom pristupu materiji je nedostatak sankcioniranja djela neovlaštenog pristupa i kompjutorske špijunaže (neovlaštenog pribavljanja podataka) kao što je to učinjeno u Njemačkoj, SAD, Kanadi, Veliko Britaniji itd. Ipak, treba spomenuti da premda ta djela nisu dio kaznenog zakona, ona jesu regulirana zakonom iz sfere trgovačkog prava (Zakonom protiv nelojalne konkurencije) sa svim posljedicama koje to sa sobom nosi (specifičnosti građanskog u odnosu na kazneni postupak).

Za očekivati je da će austrijski kazneni sutav teško odgovoriti na izazove kompjutorskog kriminaliteta ne sankcionira li uskoro i preostala kaznena djela vezana uz kompjutorski kriminalitet, pogotovo djela neovlaštenog pristupa i neovlaštenog pribavljanja tuđih podataka.

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

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.)

1990. ipak donešen je i Computer Misuse Act, kojim su u kazneno zakonodavstvo uvedena konkretna kaznena djela kompjutorskog kriminaliteta.[5] Budući da je Computer Misuse Act 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). Posjednje 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.

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 pistup učinjen sa 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

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

premještanje, korištenje ili ispisivanje sa kompjutora na kojem se nalaze na bilo koju lokaciju ili način[6].

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 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[7]. Vrlo česti primjeri ovakvih djela su slučajevi hakera koji prilikom neovlaštenog pristupa kopiraju datoteke s brojevima kreditinih kartica. Pri tome uopće nije bitno da li je dalje kazneno djelo (prijevare, krivotvorenja) izvršeno.

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 bio je Christoper Pile, aka Black Baron, autor virusa Queeg i Pathogen, koji je svojim djelovanjem nanio štete u iznosu preko milijun funti.

[6] Doc.dr.sc. Dražen Dragičević, "Kompjutorski kriminalitet i računalni sustavi", str. 162
[7] Doc.dr.sc. Dražen Dragičević, "Kompjutorski kriminalitet i računalni sustavi", str. 163

Što je sa usuglašenošću ovog zakona i Konvencije o kibernetičkom kriminalu? Iako inkrimimnacije nisu sistematizirane na isti način, sva potrebna kaznena djela su tu. Budući da je Ujedinjeno kraljevstvo država sa common law pravnim sustavom, poput Sjedinjenih država i drugih država Commonwealtha, konkretni doseg ovog propisa će ovisiti o sudovima koji će ga primjenjivati. Sudovi u common law sustavima imaju kreatornu ulogu, a njihove odluke (presedani) su bitan, stvarajući, izvor prava. Iako je 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 je 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[8]

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 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[9]

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

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 definitivno je značajan izvor podataka i iskustva kako za druge common law sustave tako i za ostale pravne sustave.

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

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[10]:

- 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 u potpunosti poštuje odredbe Konvencije o kibernetičkom kriminalu, budući da Code Penale sadrži sva kaznena djela koja je Konvencija o kibernetičkom kriminalu inkriminirala. Ovo ne iznenađuje previše, jer riječ je o zemlji koja ima snažnu zakonodavnu aktivnost, i koja je uvijek među prvima sankcionirala utjecaj novih tehnologija[11]. Pogotovo je to točno u građanskopravnoj sferi, gdje se, npr. kod problema odgovornosti tvrtki pružatelja Internet usluga često citira francuska zakonodavna i sudska praksa.

[10] **Handbook of Legislative Procedures of Computer and Network Misuse in EU Countries for assisting Computer Security Incident Response Teams (CSIRTs), str. 47**

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

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[12]

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 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.

[12] Handbook of Legislative Procedures of Computer and Network Misuse in EU Countries for assisting Computer Security Incident Response Teams (CSIRTs), str. 72

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).

Inkriminacije iz 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[13]
- 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 jaznenog djela. Tradicionalan europski pristup, na određen način potvrđen u Konvenciji o kibernetičkom kriminalu ovdje, ipak, smatram ima prednost.

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

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)

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 pregled 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.[14]

[14] Tekst Zakona o autorskom pravu : http://www.cric.or.jp/cric_e/clj/clj.html

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[15]) 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.)

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 nevedena 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

[15] http://www.4law.co.il/316.pdf

kaznenih djela prijevare, i prijevare počinjene putem računala) može unijeti nepotebnu 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 du 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 SRBIJI i CRNOJ GORI

Najnovijim izmjenama i dopunama Krivičnog zakona Srbije, izvršenim početkom 2003 (Službeni glasnik SRS 80/2002 i 39/2003) uvedeno je 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 zastićenom 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[16]. Hrvatsko kazneno pravo, od donošenja Kaznenog zakona, već sadrži većinu inkriminacija pojavnih oblika kompjutorskog kriminaliteta, a preostale, poput kaznenog djela onemogućenja ispravnog rada računala biti će unesene novom dopunom Kaznenog zakona koja je već u postupku donošenja.

Što je sa 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.

[16] http://www.projuris.org/aktuelno_comp_kriminal.htm

10. 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[17].

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[18]. 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). Zanimljivo je da je već tada u čl 309. bila sankcionirana izrada i upotreba malicioznih programa koji mogu poslužiti za neovlašteni pristup ili bilo koje drugo kazneno djelo vezano za upotrebu računala.

Prema nekim podacima, objavljenima i u glasilu udruge Business Software Alliance (BSA) i srpskog časopisa Ekonomist[19] 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 2001. 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 gotovo sve zahtjeve Konvencije o kibernetičkom kriminalu. Ono što je još preostalo ispuniti su kaznenopravno sankcioniranje kaznenih djela usmjerenih na ometanje normalnog rada kompjutorskih sustava kao i kaznenog djela neovlaštenog presretanja podataka.

[17] Register predpisov Slovenije, Ur.l. RS, št. 23/99, čl.225
[18] http://www.aas.si/pravni-viri/kzrs-fr1.html
[19] http://www.ekonomist.co.yu/magazin/ebit/12/por/slovenc.htm

11. KAZNENOPRAVNO ZAKONODAVSTVO U HRVATSKOJ

Kao i uvijek, hrvatski pravni sustav osluškuje promjene u pravnim poretcima temalja istovrsnog nam pravnog kruga. Suprotno mišljenju šire populacije, vjerujem da se većina stručnjaka slaže 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. Zato ne iznenađuje da se, kad se govori o odgovornosti pružatelja Internet usluga kod nas, ta odgovornost razmatra u okviru propisa generalne prirode, kao što je Kazneni zakon iz 1998., sa svojim izmjenama i dopunama, te leges speciales, ovisno o kojim povredama je riječ (naravno, Zakon o autorskom pravu, odredbe Zakona o obveznim odnosima).

Članci Kaznenog zakona koji u nas inkriminiraju ponašanja specificirana kao kaznena djela u člancima 2. do 6. Konvencije o kibernetičkom kriminalu su čl. 223, Oštećenje i upotreba tuđih podataka, koji pokriva kaznena djela Neovlaštenog pristupa i Oštećenja, izmjene i uništenja podataka (čl. 2 i 4. Konvencije).

Što se tiče čl. 3 i Kazneno djelo neovlaštenog presretanja podataka (Illegal Interception) u teoriji se smatra da premda čl. 223. ne sadrži odredbe o kompjutorskoj špijunaži, postoji dovoljno postojećih inkriminacija kojima se može sankcionirati ovakvo ponašanje u svojim pojavnim oblicima. Tako npr. inkriminacije o izdavanju i neovlaštenom pribavljanju poslovne tajne (čl. 295 KZ) ili odavanju službene tajne (čl. 132 KZ), odavanju državne tajne (čl. 144 KZ). Tu je i čl.133 i Nedozvoljena upotreba osobnih podataka, čime se pokriva kako prikupljanje, obrađivanje i korištenje osobnih podataka građana, tako i njihovo korištenje suprotno zakonom dozvoljenoj svrsi njihovog prikupljanja[20].

Naravno, i glava kaznenih djela protiv imovine nadopunjena je inkriminacijama koje mogu poslužiti i za sankcioniranje nekih zloporaba Interneta. Tako su tu navedena kao inkriminacije slijedeća djela:

- Povreda prava autora ili umjetnika izvođača
- Neovlaštena upotreba autorskog djela ili izvedbe umjetnika izvođača
- Oštećenje i upotreba tuđih podataka

[20] Doc.dr.sc. Dražen Dragičević: "Kompjutorski kriminalitet i informacijski sustavi", str .181 i 186.

Ovo posljednje kazneno djelo pogotovo je interesantno, jer je ovdje riječ o sasvim novom kaznenom djelu kojim se zaštićuju automatski obrađeni podaci ili kompjutorski programi, a inkriminira se i sam pristup njima pod uvjetom da su zaštićeni posebnim mjerama (šiframa)[21].

Premda navedene inkriminacije pokrivaju veliki broj zloporaba Interneta i računala, zakonodavac je mogao i trebao naći i mjesta za sankcioniranje djelovanja malicioznih programa, što bi direktno pomoglo i formiranju pravnog okvira za izražavanje odgovornosti proizvođača. Trebalo se naći i mjesta i za neovlašteno mijenjanje sadržaja tuđih Web stranica, kao i prezentaciju raznih štetnih sadržaja (dječja pornografija, zabrana veličanja nacističkih i fašističkih ideologija odredbama koje recimo imaju Austrijanci).

Ovakav trenutni pravni režim glede odgovornosti pružatelja Internet usluga smjestio bi nas, po Sieberovom tumačenju[22], u grupu zemalja koje se oslanjaju na svoje opće kaznene norme, u nedostatku specifičnih rješenja. Sieber smatra da je upotreba općeg sustava kaznenih normi i građanskopravnih normi dobro "vatrogasno" rješenje, ali da načelo pravne sigurnosti će s vremenom ipak postulirati donošenje jasnih specijalnih rješenja, budući da je riječ o pravno-tehničkoj problematici visoke složenosti koju je bolje zakonom čvrsto definirati nego ostaviti sudovima i općim propisima. Kao što je to u svom pregledu i pokazao, više je nego očito da razmatranja ovog njemačkog stručnjaka ponovo dobro odgovaraju i našoj situaciji.

Početkom srpnja 2003. donešena je novela Kaznenog zakona koja će se primjenjivati od 1.12. 2003. Ovom novelom čl. 223 je doživio veliku izmjenu, i sad se zove Povreda tajnosti, cjelovitosti i dostupnosti računalnih podataka, programa ili sustava i pokriva (obuhvaća) sve odredbe poglavlja Konvencije o tajnosti, nepovredivosti i dostupnosti podataka spremljenih na računalima i samih računala. Kza ova kaznena djela biti će kažnjiv i pokušaj.

Čl. 223 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

[21] Doc.dr.sc. Dražen Dragičević: "Kompjutorski kriminalitet i informacijski sustavi", str .184.

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.

(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.

[22] Prof. Dr. Ulrich Sieber : Responsibility of Internet Providers, str. 35

III. OSVRT NA ODGOVORNOST ISP-ova

Internet 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 i sive zone pravno nereguliranog ili konfliktno reguliranog. 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 u vlastitoj domeni, znači formalnom "teritoriju" unutar Interneta nad kojim imaju nadležnost, filtriraju promet vlastitih korisnika prema serverima u drugim domenama, znači "slobodnom" Internetu.

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[23] 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 supra bilo nešto riječi:

- 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

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

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 HT, da nabrojimo samo poznatije) te različite ustanove poput vojske i obrazovnih institucija širom svijeta (kod nas CARNet, Hrvatska Akademska Računalna Mreža). Načelno svi ISP-ovi imaju organiziranu službu za zaprimanje i obradu sigurnosnih incidenata sa ovlastima da upozori korisnike-počinitelje i uskrati im dalji pristup.

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[24] u kojem ona poseban naglasak stavlja na kaznene odredbe austrijskog Kaznenog zakona (St.G.B.) i Zakona o kaznenom postupku (St.P.O).

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

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". [25] 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 prikaz 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 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. Malo je simptomatično što su gotovo dvije godine nakon potpisivanja konvenciju ratificirale samo Hrvatska, Estonija i Albanija, od preko trideset potpisnika. Tome u prilog ide i priličan broj rezervi (članci - odredbe Konvencije koje se mogu, ali 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. Konvencija još nije stupila na snagu jer, kako je već navedeno, traži se barem pet potpisnika od kojih tri trebaju biti članovi vijeća Europe.

[25] **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."

Komparativno pravo – Francuska

Kao jedna od vodećih zemalja kontinentalnog pravnog kruga, ali i tehnološki avangardna nacija, Francuska se rano susrela sa 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 sadržaje, koje korisnici postave u obliku web stranica, datotečnih repozitorija ili oglasnih ploča (foruma), zainteresiranima Internetu.[26]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.

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 sa 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 sa 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

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

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. [27]

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

Komparativno pravo – Austrija

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

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

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[28].

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 odgovorno sti 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.[29]

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[30]. Po mišljenju G. Schmölzer, Austriji tu još treba jasno zakonsko utvrđivanje dužnosti nadzora i njenih daljih učinaka.

[28] Gabrielle Schmölzer : Internet i kazneno pravo, prijevod u Hrvatskom ljetopisu za kazneno pravo vol.4 2/97, str. 895.
[29] Prof. Dr. Ulrich Sieber : Responsibility of Internet Providers, str. 14
[30] Gabrielle Schmölzer : Internet i kazneno pravo, prijevod u Hrvatskom ljetopisu za kazneno pravo vol.4 2/97, str. 897

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

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[31].

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 sa 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 odstranjenje određenog sadržaja. . Od strane koja smatra da su joj prava povrijeđena traži se:

[31] Prof. Dr. Ulrich Sieber : Responsibility of Internet Providers, str. 17

1) potpisani zahtjev kojim se traži odstranjenje spornog materijala
2) dovoljno podataka da se može ustanoviti o povrijedi 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[32]

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.

Dalje odredbe koje su od važnosti za temu ovog rada i dodatno ograničenje odgovornosti za sveučilišta kao pružatelje Internet usluga. Zakon jasno kaže da ne postoji obveza na strani pružatelja usluge da aktivno sudjeluje 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.[33]

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

IV. 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 sa visokim stupnjem Internet penetracije, poput SAD, Francuske i Njemačke, sasvim očekivano prednjače i zakonodavnim rješenjima i praksom. Svojevrsno je iznenađenje nešto slabije stanje u Japanu. Zemlje naše neposredne okoline, nastale raspadom bivše zajedničke države, uključivši i Hrvatsku, učinile su posljenjih 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 raširenо. Konkretan dokaz ovoj tvrdnji je i izvješće BSA za državu Srbiju i Crnu Goru u kojem se ta zemlja (savim očekivano) svrstava u vrh europskih zemalja po raširenosti piratiziranog softvera, premda dotična država ima sasvim moderna zakonska rješenja za borbu protiv piratstva i drugih oblika kompjutorskog kriminaliteta. Nešto slično vrijedi i za Hrvatsku, o čemu je više riječi bilo u dijelu posvećenom hrvatskom zakonodavstvu i iskustvima.

Zaista, većina zemalja posjeduje ili će uskoro posjedovati potreban zakonski okvir za borbu protiv cyber-crimea, no ono što još uvijek ne daje povoda mirnom snu je organizacija službi unutar i izvan policijskih snaga i drugih organa reda u navedenim zemljama koje bi trebale biti najisturenije državne ustanove u borbi sa 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. Dok, dakle, praksa ne sustigne zakonodavnu djelatnost, kasniti će i informatizacija naše i okolnih država i pripadajućih gospodarstava. Odgovarajuće obrazovanim i sposobnim stručnjacima povjerena provedba odredaba Konvencije o kibernetičkom kriminalu osigurati će sigurnost i mogućnost razvoja industrije i uslužnih djelatnosti baziranih na modernoj informacijskoj

tehnologiji, a ako Hrvatska u tome odmakne naprijed, poput Slovenije, lakše će razviti svoju i privući stranu tehnološki naprednu industriju.

DODATAK:

Tablica 1.

	KAZNENA DJELA PO CYBERCRIME CONVENTION* 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	X	√	√	√	√
Austrija	√[34]	√	√	X	X
V. Britanija	√	√	√	√	√
SAD	√	√	√	√	√
Francuska	√	√	√	√	√
Švedska	X	X	√	√	X
Japan	√	√	√	X	X
Kina	√	√	√	√	√
Srbija i CG	√	√	√	√	√
Slovenija	√	√	√	√	X
Hrvatska	√	√	√	√[35]	√[36]

Tablica 1. - 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)

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

[35] i [36] Novela Kaznenog zakona donešena u srpnju 2003. i koja stupa na snagu 1. prosinca 2003. obuhvaća i preostale inkriminacije, potpuno usuglašujući Kazneni zakon s odredbama Konvencije

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)

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. http://www.usdoj.gov/criminal/cybercrime/fedcode.htm - popis federalnih propisa vezanih za kompjutorski kriminalitet.
6. Handbook of Legislative Procedures of Computer and Network Misuse in EU Countries for assisting Computer Security Incident Response Teams (CSIRTs)
7. http://www.isc.meiji.ac.jp/~sumwel_h/Codes/comp-crim.htm - zbirka relevantnih japanskih propisa
8. Tekst Zakona o autorskom pravu : http://www.cric.or.jp/cric_e/clj/clj.html - tekst japanskog zakona o autorskom pravu
9. http://www.projuris.org/aktuelno_comp_kriminal.htm članak o srpskom zakonodavstvu i komojutorskom kriminalitetu
10. Službeni glasnik Srbije SRS 80/2002 i 39/2003 – srpski Krivični zakon
11. Register predpisov Slovenije, Ur.l. RS, št. 23/99, čl.225 slovenski Kazenski zakonik
12. http://www.aas.si/pravni-viri/kzrs-fr1.html o zaštiti autorskih prava u slovenskom kaznenom zakoniku
13. http://www.ekonomist.co.yu/magazin/ebit/12/por/slovenc.htm